University of Baltimore Law Review

Volume 50 | Issue 1 Article 2

10-1-2020

Surveilling the Digital Abortion Diary

Cynthia Conti-Cook

SURVEILLING THE DIGITAL ABORTION DIARY

Cynthia Conti-Cook*

INTRODUCTION[1]

In 2017, along with her stillborn fetus, Latice Fisher, a Black woman, arrived at the Oktibbeha County General Hospital in Starkville, Mississippi[2] in an ambulance.[3] While receiving care from

---

* Cynthia Conti-Cook is a civil rights attorney and researcher based in New York City studying how technology impacts various fights for justice. She is currently on sabbatical from The Legal Aid Society's Special Litigation Unit, working as a Technology Fellow at the Ford Foundation. She is grateful to the *Univ. of Baltimore Law Review* and the Applied Feminism and Privacy Conference of 2020, Michele Gilman, and Margaret Johnson, for inviting her to publish this Article. She is also appreciative of the patient and diligent student editors working through challenging circumstances. As always, this Article has evolved through dialogue with many of my colleagues, friends, and family. Cynthia extends her appreciation for reviewing drafts, sharing edits, and extensive brainstorming to Tanya Coke, Brook Kelly-Green (who also initially drafted Parts I and Part IIA), Lynn Paltrow, Logan Koepke, Jerome Greco, Rashida Richardson, Sara Ainsworth, Indra Lusero, and Terri Rosenblatt. *The views and opinions expressed herein are solely those of the author and do not reflect and are not attributable in any way to those of the Ford Foundation.*

1. In 2005, filmmaker Penny Lane released The Abortion Diaries (2005) to "dispel[] the stigma of abortion" by inviting 12 women to speak candidly about their abortion experiences. Penny Lane, *The Abortion Diaries (2005)*, PENNY LANE, http://pennylaneismyrealname.com/film/the-abortion-diaries-2005/ [https://perma.cc/FXH3-4U3S] (last visited Nov. 3, 2020). In 2013, storyteller Melissa Madera founded The Abortion Diary podcast to "speak out against the shame, stigma, secrecy, and isolation surrounding abortion by generating, sharing, and receiving personal stories." *Mission: The Abortion Diary*, ABORTION DIARY, https://www.theabortiondiary.com/mission [https://perma.cc/7DFX-RCMH] (last visited Nov. 3, 2020). Both pieces begin with the same fundamental observation: because abortion is often stigmatized, people who have experienced it tend to prefer it remain private and, if choosing to share that experience, must feel safe and supported in doing so. *See id.*
2. Nine history scholars from Mississippi University's Department of History created "A Shaky Truce" a website that "highlights the civil rights struggles that took place in Starkville, Mississippi during the 1960s and 70s, a time when local African Americans demanded equality for all citizens." *The Project*, STARKVILLE C.R., https://starkvillecivilrights.msstate.edu/wordpress/the-project/ [https://perma.cc/PX3Y-3K7N] (last visited Nov. 3, 2020). It describes Oktibbeha County as having "a majority African American population in 1840 and continued to have one until 1950." *The Place*, STARKSVILLE C.R., https://starkvillecivilrights.msstate.edu/wordpress/the-place/ [https://perma.cc/ZM7D-GW4C] (last visited Nov. 3, 2020). The county's Black population decreased to 34.6% in 2013 and its residents remain racially segregated. *See id.*
3. Ryan Phillips, *Infant Death Case Heading Back to Grand Jury*, STARKVILLE DAILY NEWS (May 8, 2019), https://www.starkvilledailynews.com/infant-death-case-heading-back-to-grand-jury/article_cf99bcb0-71cc-11e9-963a-eb5dc5052c92.html [https://perma.cc/9H7B-CA8X] ("Fisher then walked out to the ambulance, was placed on a stretcher, and transported to OCH Regional Medical Center in Starkville where she was evaluated and questioned by hospital staff. Prosecutors allege that Fisher

medical staff, she was also immediately treated with suspicion of committing a crime.[4] Her statements to nurses, the medical records, and the autopsy records of her fetus were turned over to the local police to investigate whether she intentionally killed her fetus.[5] To develop these records into evidence supporting an indictment for intentional murder, prosecutors would need some evidence about Ms. Fisher's intent.[6] This is typical; at best, prosecutions of people based on their pregnancy outcomes usually rely on circumstantial medical evidence, what patients report to nurses and doctors, and cooperation from medical staff.[7] Without a confession, a diary, or something similar, direct evidence of a person's mindset or intentions prior to a termination is usually absent.[8] The lack of "intent" evidence might not discourage a prosecutor from attempting to indict someone, but it might dissuade a grand jury from voting for an indictment.[9] In Ms. Fisher's case, the prosecutor sought to fill that gap in the initial presentation to the Grand Jury by arguing that Ms. Fisher's web search history proved her criminal intent; it included searches for how to induce a miscarriage and evidence that she purchased misoprostol online.[10] The first Grand Jury was convinced and indicted Ms. Fisher for second degree murder.[11]

---

admitted to a nurse that she learned she was pregnant during an annual gynecological exam a month earlier, but she failed to make any follow-up appointments for an ultrasound or other prenatal care. . . . Fisher was interviewed by investigators about how the events occurred and court documents say she admitted that she didn't want any more children, that she couldn't afford any more and that she 'simply couldn't deal with being pregnant again.' Investigators also learned that on April 17, 2017, which was far into Fisher's third trimester, she researched medication abortion. This information came after investigators downloaded Latice Fisher's cell phone memory and data, which revealed her internet search history. She also admitted to conducting internet searches, including how to induce a miscarriage, 'buy abortion pills, mifeprisone online, misoprostol online,' and 'buy Misoprostol abortion pill online.' Fisher then purchased misoprostol following the online search, according to the district attorney's office.").

4. *See id.*
5. *Id.*
6. *See* Rodgers v. State, 166 So. 3d 537, 547 (Miss. Ct. App. 2014).
7. *See*, *e.g.*, Phillips, *supra* note 3.
8. *See*, *e.g.*, *id* (detailing prosecutorial reliance on search history and statements to medical professionals).
9. *See*, *e.g.*, *id.*
10. *Id.* Some of the searches Ms. Fisher entered were as follows: "'buy abortion pills, mifeprisone online, misoprostol online,' and 'buy Misoprostol abortion pill online.'" *Id.*
11. *Id.* Ms. Fisher's first indictment was voluntarily dismissed by the prosecutor after her defense team—the National Advocates for Pregnant Women and local counsel Williams Starks—presented the District Attorney with expert opinions which cast a

This Article presents a sobering forecast; the inclusion of Ms. Fisher's alleged internet search history related to her reproductive health as evidence of criminal intent will become standard protocol across the country once abortion is again criminalized.[12] Restricted access to abortion clinics[13] and an increasing number of Americans turning to the internet for medical advice[14] are both contributing to

---

doubt on the conclusions reached by the state medical examiner; even still, the District Attorney again presented the case against Ms. Fisher unsuccessfully in March 2020. Lauren Rankin, *How an Online Search for Abortion Pills Landed This Woman in Jail*, FAST CO. (Feb. 26, 2020), https://www.fastcompany.com/90468030/how-an-online-search-for-abortion-pills-landed-this-woman-in-jail [https://perma.cc/R6EL-WFA6]; *see also* A No Bill, Mississippi v. Fisher Grand Jury No. 165 (Mar. 6, 2020) (on file with the author) (grand jury document filed in The Circuit Court of Oktibbeha County, Mississippi).

12. *See infra* Part III.

13. RACHEL K. JONES ET AL., ABORTION INCIDENCE AND SERVICE AVAILABILITY IN THE UNITED STATES, 2017 1 (Guttmacher Inst., 2019), https://www.guttmacher.org/sites/default/files/report_pdf/abortion-incidence-service-availability-us-2017.pdf [https://perma.cc/3T9A-76WJ] ("[R]egional and state disparities in clinic availability grew more pronounced; the number of clinics increased in the Northeast and the West, by 16% and 4% respectively, and decreased in the Midwest and the South, by 6% and 9%, respectively."); Elizabeth Nash et al., *State Policy Trends 2019: A Wave of Abortion Bans, but Some States Are Fighting Back*, GUTTMACHER INST. (Dec. 10, 2019), https://www.guttmacher.org/article/2019/12/state-policy-trends-2019-wave-abortion-bans-some-states-are-fighting-back# [https://perma.cc/U2V8-52YU] ("In 2019, conservative state legislators raced to enact an unprecedented wave of bans on all, most or some abortions, and by the end of the year, 25 new abortion bans had been signed into law, primarily in the South and Midwest. Along with this new strategy, legislators also continued their efforts to adopt other types of abortion restrictions, including requirements for abortion providers to give patients misleading and inaccurate information about the potential to reverse a medication abortion as part of abortion counseling."); Elizabeth Nash, *A Surge in Bans on Abortion as Early as Six Weeks, Before Most People Know They Are Pregnant*, GUTTMACHER INST., https://www.guttmacher.org/article/2019/03/surge-bans-abortion-early-six-weeks-most-people-know-they-are-pregnant [https://perma.cc/8JRP-HENW] (May 30, 2019) ("On May 30, Louisiana became the fifth state this year to enact a ban at six weeks of gestation, before many people even know that they are pregnant. The other four states where six-week bans have been signed into law in 2019 are Georgia, Ohio, Kentucky and Mississippi. In addition, Alabama enacted a near-total abortion ban, while Missouri enacted a ban at eight weeks of gestation. None of these laws are currently in effect.").

14. *See* Pete Roseler, *New Research Shows Why Doctors Need a Strong Online Presence*, INC. (May 21, 2018), https://www.inc.com/peter-roesler/new-research-shows-why-doctors-need-a-strong-online-presence.html [https://perma.cc/Y4UV-SBEX] ("A survey of more than 1,700 U.S. adults found the four out of five (80 percent) respondents have used the internet to make a healthcare-related search in the past

how pregnant people increasingly identify their options with respect to their reproductive health online, creating a trail of digital evidence.[15] These digital trails are already being introduced as evidence against them in criminal cases for intentionally terminating their pregnancies.[16] If the United States Supreme Court votes to overturn *Roe v. Wade* and a number of state legislatures vote to criminalize abortion, investigations and prosecutions of pregnancy outcomes will increasingly rely on these unprotected digital trails.[17]

In addition to facilitating prosecutions of pregnant people for intentionally terminating their pregnancies, technology will also enhance the government's ability to surveille, investigate, and prosecute pregnant people who did not seek to terminate but whom the state seeks control over by virtue of their pregnancy status.[18] For example, pregnant people's decisions—to self-medicate, to not medicate, to seek substance abuse treatment, to drink alcohol, or smoke cigarettes—are all decisions that could be criminalized and potentially surveilled digitally.[19] A wide variety of digital forensic

---

year. . . . [and] three in five (63 percent) of all the respondents will choose one provider over another because of a strong online presence.").

15. *See infra* Part III.

16. *See infra* Part III. This Article does not argue or consider the status of self-induced abortions as a fundamental right. While it has been argued to the contrary, that argument is worth revisiting given new abortion pill technology. *See* Suzanne M. Alford, *Is Self-Abortion a Fundamental Right?*, Note, 52 DUKE L.J. 1011, 1021 (2003); *see also* Becky Little, *The Science Behind the "Abortion Pill"*, SMITHSONIAN MAG. (June 23, 2017), https://www.smithsonianmag.com/health-medicine/science-behind-abortion-pill-180963762/ [https://perma.cc/Q8PJ-WLLA]. Marissa Kreutzfeld doesn't address this in her argument, instead saying that the environment of restricted access alone should change Alford's type of analysis. Marissa Kreutzfeld, *An Unduly Burdensome Reality: The Unconstitutionality of State Feticide Laws That Criminalize Self-Induced Abortion in the Age of Extreme Abortion Restrictions*, 38 WOMEN'S RTS. L. REP. 55, 104 (2016); Andrea Rowan, *Prosecuting Women for Self-Inducing Abortion: Counterproductive and Lacking Compassion*, 18 GUTTMACHER POL'Y. REV. 70, 70–71 (2015).

17. *See supra* notes 12–16 and accompanying text.

18. Kira Proehl, *Pregnancy Crimes: New Worries to Expect When You're Expecting*, 53 SANTA CLARA L. REV. 661, 681 (2013) ("Virtually every action a pregnant woman takes can have an impact on her fetus. If states choose to hold women criminally liable for the outcomes of their pregnancies, where should society draw the line between acceptable and unacceptable behavior? The difficulty underlying this determination has historically led courts to be reluctant to prosecute women for harm to their fetuses resulting from certain acts or omissions. If states are serious about prosecuting pregnancy crimes, how should the law define 'good' versus 'bad' maternal behavior?").

19. AMNESTY INT'L, CRIMINALIZING PREGNANCY: POLICING PREGNANT WOMEN WHO USE DRUGS IN THE USA 20 (2017), https://www.amnesty.org/download/Documents/AMR5

technology and other forms of technology broaden state surveillance power through online searches, geofencing,[20] location tracking, purchasing history, and more.[21] Combined, these data points could identify, for example, the profiles of pregnant people spending time at substance abuse treatment centers, making purchases at bars, or repeatedly taking a particular route across state lines.[22] Digital surveillance through location-tracking data embedded on smartphones and various applications (apps) was widely introduced during the outbreak of the COVID pandemic to enforce social distancing orders, trace contact with people who were presumed to have COVID, and investigate quarantine violations.[23] Any number

---

162032017ENGLISH.pdf [https://perma.cc/5ZB3-GWY3] ("Some localities have chosen to pursue certain conduct more aggressively than others, for example, deciding to remove children solely based on marijuana use, while others do not pursue or ignore these cases altogether. In most states, a CPS worker may use a single positive drug test to make a claim of abuse even without an assessment of the family's ability to care for a child. Even in states without such laws defining drug exposure during pregnancy as child abuse, CPS can monitor pregnant women and intervene as soon as a child is born.") (footnotes omitted); Lynn M. Paltrow & Jeanne Flavin, *Arrests of and Forced Interventions on Pregnant Women in the United States, 1973–2005: Implications for Women's Legal Status and Public Health*, 38 J. HEALTH POL., POL'Y & L., 299, 314 (2013) ("Declining a 'biophysical profile' at a prenatal care appointment a week earlier, as well as drinking alcohol and smoking cigarettes while pregnant, all legal activities, were mentioned in the criminal complaint describing the grounds for her arrest on charges of attempted first-degree intentional homicide and first-degree reckless injury.").

20. Proximi.io, *What are Geofences? - All About Geofencing in 5 Min*, YOUTUBE (Feb. 26, 2018), https://www.youtube.com/watch?v=oklOTx_jnbA; Sarah K. White, *What is Geofencing? Putting Location to Work*, CIO (Nov. 1, 2017, 12:43 PM), https://www.cio.com/article/2383123/geofencing-explained.html [https://perma.cc/Y8EN-TNHY] ("Geofencing is a service that triggers an action when a device enters a set location.").
21. *See* Paige M. Boshell, *The Power of Place: Geolocation Tracking and Privacy*, A.B.A.: BUS. L. TODAY (Mar. 25, 2019), https://businesslawtoday.org/2019/03/power-place-geolocation-tracking-privacy/ [https://perma.cc/FJF4-L8LK].
22. Charles Blain, *Police Could Get Your Location Data Without a Warrant. That Has to End*, WIRED (Feb. 2, 2017, 7:00 AM), https://www.wired.com/2017/02/police-get-location-data-without-warrant-end/ [https://perma.cc/BU3F-WL6V] ("Your cell phone records every location you visit if the phone's location services are turned on, which is more often than not. Called cell-site location information, this data is tracked on both Android devices and iPhones. The information can be quite telling; it might show the location of your home, your office, and other places you visit often. The problem is that it can teach police about a person's behavior and then can be used against them.").
23. Yingzhi Yang & Julie Zhu, *Coronavirus Brings China's Surveillance State Out of the Shadows*, REUTERS (Feb. 7, 2020, 7:20 AM), https://www.reuters.com/article/us-china

of "bad behaviors" by pregnant people could similarly be surveilled with a range of available technology.[24] Depending on the inclinations of the prosecutor and the laws in each state, people could potentially be criminalized for being pregnant and doing or refusing to do something that is perceived as creating a risk of harm to fetuses.[25] Indeed, many prosecutors have already charged people for conduct that would be legal but for their pregnancy.[26] How

-health-surveillance-idUSKBN2011HO [https://perma.cc/4EZY-WFSY] ("Artificial intelligence and security camera companies boast that their systems can scan the streets for people with even low-grade fevers, recognize their faces even if they are wearing masks and report them to the authorities. If a coronavirus patient boards a train, the railway's 'real name' system can provide a list of people sitting nearby. Mobile phone apps can tell users if they have been on a flight or a train with a known coronavirus carrier, and maps can show them locations of buildings where infected patients live."); Mark Gurman, *Apple, Google Bring Covid-19 Contact-Tracing to 3 Billion People*, BLOOMBERG (Apr. 10, 2020, 7:53 PM), https://www.bloomberg.com/news/articles/2020-04-10/apple-google-bring-covid-19-contact-tracing-to-3-billion-people [https://perma.cc/P2ZN-RKNH] ("Apple Inc. and Google unveiled a rare partnership to add technology to their smartphone platforms that will alert users if they have come into contact with a person with Covid-19. People must opt in to the system, but it has the potential to monitor about a third of the world's population."); Byron Tau, *Government Tracking How People Move Around in Coronavirus Pandemic*, WALL ST. J. (Mar. 28, 2020), https://www.wsj.com/articles/government-tracking-how-people-move-around-in-coronavirus-pandemic-11585393202 [https://perma.cc/C994-YUFP] ("The federal government, through the Centers for Disease Control and Prevention, and state and local governments have started to receive analyses about the presence and movement of people in certain areas of geographic interest drawn from cellphone data. . . .").

24. Proehl, *supra* note 18, at 682 ("Where states are choosing to draw the line between 'good' and 'bad' behavior appears to be rather arbitrary. If states are truly worried about what pregnant women are doing to affect fetal health, should not women be prevented from participating in any activity that is known to have a negative impact? In *What to Expect When You're Expecting*, the authors warn women to avoid activities like changing a cat's litter box, eating unpasteurized cheese, sushi or deli meats, gardening without gloves, handling household cleaning products, and drinking coffee—all of which can impact a fetus. Under South Carolina law, a woman is guilty of homicide by child abuse if she causes death 'while committing child abuse or neglect, and the death occurs under circumstances manifesting an extreme indifference to human life.' If a woman knows that garden chemicals are bad for her developing fetus, yet decides to work in a garden without wearing appropriate gloves, this could easily be seen as a 'conscious failure to exercise due care' regarding the safety of her fetus. Under existing law, she could be found criminally liable for her actions if something during her pregnancy brings her case to the attention of state prosecutors.") (footnotes omitted).

25. *Id.*

26. AMNESTY INT'L, *supra* note 19, at 20; Paltrow & Flavin, *supra* note 19, at 314 ("Declining a 'biophysical profile' at a prenatal care appointment a week earlier, as well as drinking alcohol and smoking cigarettes while pregnant, all legal activities,

technology will enhance the potential for criminalizing "bad behaviors" unrelated to abortion—i.e., changing a cat's litter box, eating unpasteurized cheese, sushi or deli meats, gardening without gloves, handling household cleaning products, and drinking coffee[27]—deserves future in-depth treatment, but is not the focus of this Article, which solely examines the role of technology in emboldening those who wish to criminalize the pregnant person for specific pregnancy outcomes.[28]

When pregnant people are criminalized—whether for decisions to terminate, for being pregnant and engaging in a specific behavior, or experiencing a condition thought to pose some risk to the pregnancy—the consequences touch all aspects of their lives, while impacting their families and communities.[29] In addition to facing time-consuming and expensive consequences (e.g., criminal conviction, owing fines and fees, potentially serving jail time, being subject to mandated programs, or required meetings with caseworkers) people who have been criminalized pay in many other ways for their convictions.[30] Pregnant people may lose custody over other family members because of a prosecution, lose work, medical care, careers, educational opportunities, stable housing, vehicles, confiscated digital devices, and many other survival tools as a result of a prosecution.[31] Digital tools—like those for risk assessments used in child welfare systems, social welfare programs, public

---

were mentioned in the criminal complaint describing the grounds for her arrest on charges of attempted first-degree intentional homicide and first-degree reckless injury.").

27. *See supra* note 24 and accompanying text.

28. *See generally infra* Part III.

29. Torrey McConnell, Comment, *The War on Women: The Collateral Consequences of Female Incarceration*, 21 LEWIS & CLARK L. REV. 493, 501 (2017) ("Because of the failure to recognize these systemic barriers, many women will be released from prison with collateral consequences that will last long beyond the completion of their sentence."). The collateral consequences include: (1) lack of appropriate treatment for mental illness and addiction; (2) lack of access to state welfare and benefits; (3) maternal incarceration and intergenerational criminality; and (4) termination of parental rights. *Id.* at 501, 504, 508, 511.

30. *See id.* at 501–13.

31. *See, e.g.*, *id.* at 509; Nicholas Freudenberg, *Adverse Effects of US Jail and Prison Policies on the Health and Well-Being of Women of Color*, 92 AM. J. PUB. HEALTH 1895, 1895 (2002); Christie Thompson, *For Tarra Simmons, Her Time in Prison Isn't a Liability. It's a Campaign-Trail Identity*, MOTHER JONES (June 23, 2020), https://www.motherjones.com/politics/2020/06/tarra-simmons-kevin-harris-formerly-incarcerated-candidates-public-office/ [https://perma.cc/T2GM-ZHXG]; Phillips, *supra* note 3.

substance abuse programs, as well as police, correctional, educational or juvenile systems—all interact with people who have prior convictions to make surveillance on supervision more scrutinizing and omnipresent, and to make access to resources more restrictive.[32] If more pregnant people are prosecuted in relation to the termination of pregnancies, their marginalization will deepen.[33] This topic also deserves further investigation as the impact of digital, biometric, and genetic surveillance accumulates to increasingly "microtarget" historically oppressed communities.[34]

This Article also examines how digital trails will lead to investigations and prosecutions of medical providers and those who assist with abortions.[35] Imagine what Jane—the underground abortion network that grew out of Chicago in the pre-*Roe* late sixties—would look like today if abortions were criminalized.[36] Instead of hanging flyers on campuses and putting advertisements in newspapers that read "Pregnant? Don't want to be? Call Jane,"[37] in today's world, there may be Instagram accounts, websites, email addresses, and a Facebook group where members connect instead of meeting in person.[38] These communication technologies have greatly

32. *See generally* Dan Hurley, *Can an Algorithm Tell When Kids Are in Danger?*, N.Y. TIMES (Jan. 2, 2018), https://www.nytimes.com/2018/01/02/magazine/can-an-algorithm-tell-when-kids-are-in-danger.html [https://perma.cc/PMT2-CGW3] (discussing the strengths and weaknesses of a novel predictive analytical algorithm used by police in Allegheny County, Pennsylvania since 2016 to predict when children collateral to criminal activity are at risk of abuse or neglect).

33. Rowan, *supra* note 16, at 70.

34. Dipayan Ghosh, *What Is Microtargeting and What Is It Doing in Our Politics?*, MOZILLA: INTERNET CITIZEN (October 4, 2018), https://blog.mozilla.org/internetcitizen/2018/10/04/microtargeting-dipayan-ghosh/ [https://perma.cc/752U-FRE3] ("Microtargeting is a marketing strategy that uses people's data — about what they like, who they're connected to, what their demographics are, what they've purchased, and more — to segment them into small groups for content targeting.").

35. *See infra* Section III.B.

36. Clyde Haberman, *Code Name Jane: The Women Behind a Covert Abortion Network*, N.Y. TIMES (Oct. 14, 2018), https://www.nytimes.com/2018/10/14/us/illegal-abortion-janes.html [https://perma.cc/L6JN-BT4Z] ("The Janes' tactics were worthy of a spy novel. A woman seeking to end her pregnancy left a message on an answering machine. A 'Callback Jane' phoned her, collected information and passed it to a 'Big Jane.' Patients would be taken first to one address, 'the front,' for counseling. They were then led, sometimes blindfolded, to another spot, 'the place,' where a doctor did the abortion.").

37. *Id.* ("The no-frills advertisement, printed at times in student and alternative newspapers, went straight to the point: 'Pregnant? Don't want to be? Call Jane.' A telephone number followed.").

38. *See, e.g.*, Lizzie Presser, *Whatever's Your Darkest Question, You Can Ask Me*, CAL. SUNDAY MAG. (Mar. 28, 2018), https://story.californiasunday.com/abortion-providers

improved access to reproductive health options and providers, but they are tools that also leave digital trails—not just to the individuals that use them, but also to the entire network with whom an individual interacts on a digital device.[39] While the analog era did not protect Jane members from eventual arrest, it did allow them to operate undetected for several years.[40] To imagine how Jane may survive in the digital era, this Article includes anatomies of various digital investigations of internet-dependent networks to extract lessons about how similar techniques may be used against online abortion pill providers, both medical and non-medical.[41]

This Article hopes to introduce some common vocabulary between communities that may not normally intersect.[42] While many terms will be defined throughout the Article, there are a few key concepts worth defining upfront. "Criminalization" is used throughout the Article to describe the process through which multiple legal, political, and social maneuvers—including some that are assisted by technology—are leveraged to punish people.[43] To the extent technology is described as criminalizing, playing a role in

---

[https://perma.cc/RX6A-MU4Q] ("Anna started posting on Facebook about abortion, looking for direction. Eventually, a friend reached out to her, offering to introduce her to a woman named Natalie. . . . After several calls, Natalie told Anna about a side of her life she hadn't yet shared: She was helping with a workshop on how to provide home abortions.").

39. *See infra* Section III.A.2.

40. Haberman, *supra* note 36 ("The network came into being in 1969. . . . In 1972, the Chicago police raided an apartment used by the Janes, and arrested seven of them.").

41. *See infra* Sections III.A.5, III.B.

42. *See supra* notes 43–52 and accompanying text.

43. *Interrupting Criminalization: Research in Action*, BARNARD CTR. FOR RES. ON WOMEN, http://bcrw.barnard.edu/fellows/interrupting-criminalization-research-in-action/ [https://perma.cc/G6B9-EE5W] (last visited Nov. 3, 2020) ("Criminalization is the social and political process by which society determines which and whose actions or behaviors will be punished by the state. At the most basic level, criminalization involves the passage and enforcement of criminal laws. While framed as neutral, decisions about what kinds of conduct to punish, how, and how much are very much a choice, guided by existing structures of economic and social inequality based on race, gender, sexuality, disability, and poverty, among others. The practice of criminalization extends beyond laws and policies to more symbolic and entrenched processes by which people are deemed categorically 'criminal.' This process is fueled by widespread and commonly accepted stereotypes, which are highly racialized and gendered—whether they are about 'thugs,' 'crack mothers,' 'welfare queens,' or 'bad hombres.' These narratives create generalized states of anxiety and fear, and brand people labeled 'criminal' as threatening, dangerous, and inhuman. In this context, restrictions on freedom, expression, movement, and survival, as well as violence, denial of protection, banishment, and exile are the inevitable and natural responses.").

criminalizing individuals, or having the effect of criminalizing more pregnant people, it is not meant to be identified as the motivating factor, nor is this argument suggesting technology should not be an important tool in helping people access information about abortions, or directly accessing medication abortions.[44] The technology at issue here—digital forensic tools and surveillance technology—is neutral to the type of offense it is deployed for; it does not have programming constraints that would only allow it to detect internet searches that only suggest, for example, homicidal intent.[45] The underlying assumption upon which all these tools were constructed is that the crimes the state is emboldened to prosecute are clearly criminal conduct, as opposed to conduct that some consider criminal and some consider associated with a fundamental right.[46]

While some have argued that self-induced abortion is not a fundamental right, presuming it to include a wide spectrum of procedures akin to self-harm (e.g., throwing oneself down the stairs, coat hanger abortions, ingesting poisons),[47] I adopt the definition of legal advocacy organization If/When/How: "[a self-induced abortion is] [a]n abortion that occurs most commonly in someone's home, done in privacy and in safety, sometimes with the help of a caregiver, friend, or family member. It may include the use of pharmaceutical pills, traditional herbs, or other means to end a pregnancy."[48] Rather than presuming self-induced abortions are unsafe, I make the assumption throughout this Article, based on numerous studies, that they are generally safe procedures that can be managed at home.[49]

---

44. *See infra* Sections III.A.1, III.A.2.
45. *See generally* Patrick Toomy, *The NSA Continues to Violate Americans' Internet Privacy Rights*, ACLU (Aug. 22, 2018), https://www.aclu.org/blog/national-security/privacy-and-surveillance/nsa-continues-violate-americans-internet-privacy [https://perma.cc/239G-5SQS].
46. *See infra* notes 66–77 and accompanying text.
47. Alford, *supra* note 16, at 1013, 1015.
48. *Compare* The SIA Legal Team, *Roe's Unfinished Promise*, IF/WHEN/HOW (2018), https://www.ifwhenhow.org/download/?key=XpBzIyAguykWnk32raFjX28RDycRiCHNDUx5tWmkJe2zr1tdJB8WitpkmyzyMMdn [https://perma.cc/VJT4-VVCC], *with* Alford, *supra* note 16, at 1012–13.
49. Abigail Aiken et al., *Self-Reported Outcomes and Adverse Events After Medical Abortion Through Online Telemedicine: Population Based Study in the Republic of Ireland and Northern Ireland*, 357 BMJ 1, 1 (May 2017) (finding that "[s]elf sourced medical abortion using online telemedicine can be highly effective, and outcomes compare favourably with in clinic protocols."); Julia Belluz, *Abortions by Mail Are Available Now in the US. Here's What You Need to Know*, VOX, https://www.vox.com/science-and-health/2018/10/20/17999996/abortion-mail-online-mifepristone-misoprostol [https://perma.cc/JU86-WWB8] (Oct. 22, 2018, 8:15 AM); WORLD HEALTH ORG., MODEL LIST OF ESSENTIAL MEDICINES 46 (2017),

Digital data (and digital evidence) is also mentioned frequently throughout the Article to reference "information and data of value to an investigation that is stored on, received, or transmitted by an electronic device."[50] It can include online browsing history, unencrypted communications, location history, purchasing history, social media activity, and health data generated by apps or added manually, for example, menstrual cycle trackers (tracking a wide variety of data, which includes moods, appetite assessments, physical symptoms, and sexual intercourse).[51] All these systems generate digital trails that could potentially be used as evidence against pregnant people and providers in prosecutions related to the terminations of their pregnancies.[52]

This Article proceeds in four parts. Part I grounds us in the long history of criminalization of specific pregnancy outcomes motivated by racism, misogyny, and maintenance of patriarchal power structures, expressed through various legal, medical, and moral distinctions regarding when a decision to terminate is criminal, and the sociocultural motivations behind criminalization.[53] Part I is intended to remind us that the conflict presented here is ancient and the corresponding solutions must match its complexity; enacting laws that respect digital rights or setting guardrails around what health-related information can be gleaned from our digital devices and used against us in criminal court is a starting point, not a conclusive victory.[54] Part II gives this problem urgency; the combination of restricted access to abortion clinics and the looming threat of the

---

http://apps.who.int/iris/bitstream/handle/10665/273826/EML-20-eng.pdf [https://perma.cc/Y4HU-28RA]; Beverly Winikoff et al., *Safety, Efficacy, and Acceptability of Medical Abortion in China, Cuba, and India: A Comparative Trial of Mifepristone-Misoprostol Versus Surgical Abortion*, 176 AM. J. OBSTETRICS & GYNECOLOGY 431, 431 (1997) ("The medical regimen had more side effects, particularly bleeding, than did surgical abortion but very few serious side effects. Failure rates for medical abortion, although low, exceeded those for surgical abortion: 8.6% versus 0.4% (China), 16.0% versus 4.0% (Cuba), and 5.2% versus 0% (India). Nearly half of failures among medical clients were not true drug failures, however, but surgical interventions not medically necessary (acceptability failures or misdiagnoses). Women were satisfied with either method, but more preferred medical abortion.").

50. SEAN E. GOODISON ET AL., DIGITAL EVIDENCE AND THE U.S. CRIMINAL JUSTICE SYSTEM 3 (2015), https://www.rand.org/content/dam/rand/pubs/research_reports/RR800/RR890/RAND_RR890.pdf [https://perma.cc/296H-939R].

51. *See infra* Section III.A.6.

52. *See infra* Section III.B.

53. *See infra* Part I.

54. *See infra* Part I.

United States Supreme Court overturning *Roe v. Wade* will result in more people relying on the internet for information related to abortion, and more people being investigated and prosecuted for conduct related to terminating their pregnancy.[55]

Part III introduces the role of technology in this emergent future.[56] It walks through the increasingly intense amount of private, medically-related information we are all sharing with our digital devices, and focuses on how this is amplified for pregnant people.[57] Part III then walks through digital forensic techniques currently used by police and prosecutors, along with two case studies of women who have been prosecuted with digital evidence extracted from their devices,[58] and two case studies of providers whose distribution of online abortion pills have resulted in a federal investigation and federal prosecution.[59] In addition to online search histories, Part III explores multiple types of digital evidence that can also be culled to support a prosecution, including location tracking data, website navigation history, purchasing history, social media activity, wearable device data, data entered into apps (e.g., menstrual cycle tracking apps), and home devices connected to the internet (e.g., Alexa, Amazon Ring, smart refrigerators, and other "smart" devices for homes).[60]

Finally, Part IV introduces various social justice movements aimed at protecting us from government collection and deployment of our data against us, reviews litigation strategies, legislative campaigns, and "digital hygiene" practices we should all share to protect ourselves and our movement networks in the face of increasing corporate and governmental data surveillance.[61]

The goal of this paper is to build increased awareness and common goals across multiple movements, help identify and mitigate risks related to relying on digital devices for information about reproductive health, to introduce new versions of old arguments to protect people from having their digital devices used against them in criminal court, to introduce defenders and technologists to

55. *See infra* Part II.
56. *See infra* Section III.A.
57. *See infra* Section III.A.
58. *See infra* Section III.B.
59. *See infra* Section III.B.1.
60. *See infra* Section III.B.2.
61. *See infra* Part IV; NACDLvideo, *Digital Hygiene for Defense Lawyers: A Digital Security Checklist [webinar]*, YOUTUBE (Oct. 2, 2019), https://www.youtube.com/watch?v=AMGKW66Hp8Y.

reproductive justice framing, and to flag the real threats that poor and low-income pregnant people of color already experience.

My hope is for this Article to help build conversations connecting digital privacy, reproductive justice, decriminalization, and anti-surveillance movements, as well as informing criminal defense practitioners about how to best protect a pregnant person's right to self-induce abortions and self-determine their reproductive decisions with any and all tools that support them, including their digital devices.

I. HISTORY OF CRIMINALIZATION OF PREGNANT PEOPLE AND PROVIDERS[62]

For much of history, abortion services were the realm of midwives—women providing services to other women through social networks—by passing along folk knowledge or providing herbal remedies that would induce termination of a pregnancy.[63] Public advertisements for tonics promoted relief from "obstruction of menstruation," as did "Female Renovating Pills."[64] The need to end a pregnancy was generally understood during a time when pregnancy and birth were considered life threatening, and social consequences for unwed mothers were severe.[65] It was not until the seventeenth century that the first attempt to criminalize self-induced abortion was documented.[66] From that point, religious and secular law evolved both in England and America regarding whether a third-party or pregnant person could be criminalized for ending a pregnancy.[67]

---

62. The first draft of Part I and Part II.A. were originally drafted by Brook Kelly-Green, who granted the author permission to use them.

63. BARBARA EHRENREICH & DEIRDRE ENGLISH, WITCHES, MIDWIVES, AND NURSES: A HISTORY OF WOMEN HEALERS 85 (2d ed. 2010) ("In 1910, about 50 percent of all babies were delivered by midwives—most were blacks or working class immigrants."); *id.* at 41 ("As for female sexuality, witches were accused, in effect, of giving contraceptive aid and of performing abortions.").

64. CARROL SMITH-ROSENBERG, DISORDERLY CONDUCT: VISIONS OF GENDER IN VICTORIAN AMERICA 219 (1985); JANET FARREL BRODIE, CONTRACEPTION AND ABORTION IN THE NINETEENTH-CENTURY AMERICA 254 (1997).

65. *See* Geoffrey Chamberlain, *British Maternal Mortality in the 19th and Early 20th Centuries*, 99 J. ROYAL SOC'Y MED. 559, 559 (2006).

66. *See* Alford, *supra* note 16, at 1019; Samuel W. Buell, Note, *Criminal Abortion Revisited*, 66 N.Y.U. L. REV. 1774, 1785 (1991).

67. *See* Alford, *supra* note 16, at 1020 ("English common law also addressed the issue of whether a woman could be held criminally liable for self-aborting after quickening. Although it has been contended that the common law did not permit punishment of women who self-aborted or submitted to abortion, there is case law to the contrary. In

With the formalization and professionalization of medicine, and the establishment of the American Medical Association in the mid-to-late 1800s, doctors maneuvered to monopolize abortion and obstetrics, lobbying to remove midwives from the practice of reproductive health and abortion through licensing regimes.[68] This was during a period marked by growing social conservatism, fears of slowing birth rates among white Americans, and reinforcement of traditional gender roles of women as wife and mother and man as husband and provider.[69] The Comstock Laws of 1873 banned the publication and dissemination of information about contraception.[70] By the end of the 19th century, every state except Kentucky had laws banning abortion, with Connecticut passing the first state law to criminalize abortion in 1821 and New York following suit in 1845.[71] Over the period leading up to the *Roe v. Wade* decision in 1973, low-income women were least able to access abortion procedures, while middle to upper class women typically accessed abortion services through private family physicians or by traveling outside of the United States to obtain the procedure.[72]

Through its decision in *Roe v. Wade*, the Supreme Court guaranteed a constitutional privacy protection to pregnant people regarding their right to make the decision to have an abortion.[73] In

---

the 1602 case of *Regina v. Webb*, a woman was indicted for self-aborting through the use of poison. Although the defendant received a general pardon—it is unclear whether she was pardoned before or after conviction—this case illustrates that, from an early point in the development of British common law, a woman could be criminally prosecuted for self-aborting.") (footnotes omitted); *id.* at 1014 (quoting State v. Ashley, 701 So. 2d 338, 340–42 (Fla. 1997)).

68. EHRENREICH & ENGLISH, *supra* note 63, at 61; Reva Siegel, *Reasoning from the Body: A Historical Perspective on Abortion Regulation and Questions of Equal Protection*, 44 STAN. L. REV. 261, 300 (1992); *see* JAMES C. MOHR, ABORTION IN AMERICA: THE ORIGINS AND EVOLUTION OF NATIONAL POLICY, 1800–1900 147 (1978).

69. *See* Siegel, *supra* note 68, at 327–28.

70. *Id.* at 314–15.

71. Alford, *supra* note 16, at 1021–22; Buell, *supra* note 66, at 1783–85. Yet even then, "the general consensus was that the woman herself was not a criminal." NAT'L INST. FOR REPRODUCTIVE HEALTH, WHEN SELF-ABORTION IS A CRIME: LAWS THAT PUT WOMEN AT RISK 1 (2017) (footnotes omitted), https://www.nirhealth.org/wp-content/uploads/2017/06/Self-Abortion-White-Paper-Final.pdf [https://perma.cc/79YN-RNFH].

72. All Things Considered, *What Abortion Was Like in the U.S. Before Roe v. Wade*, NPR (May 20, 2019, 5:26 PM ET), https://www.npr.org/2019/05/20/725139713/what-abortion-was-like-in-the-u-s-before-roe-v-wade [https://perma.cc/5TW7-JLW7] (discussing the dangers women faced in receiving illegal abortions prior to the Supreme Court decision in *Roe v. Wade*, 410 U.S. 113 (1973)).

73. *See* 410 U.S. at 153–54.

the following few years, Congress passed the so-called Hyde Amendment to ban federal funding for abortion services, summarily creating an economic, and in many cases, a racial divide between women who can and cannot afford to access abortion.[74] In addition, pregnant people have continued to be criminalized for a wide variety of conduct related to their bodies during their pregnancy, including drug use, refusal of medical treatments and interventions during pregnancy and birth, and decisions to intentionally terminate a pregnancy outside of a traditional medical setting.[75] Most individuals targeted for criminalization are low-income women, women of color, immigrant women, and those at the intersections of these characteristics.[76] This pattern demonstrates the persistence of misogyny and racism at play in legal systems that seek to regulate the decisions women make about their bodies.[77]

II. CURRENT LANDSCAPE

A. Increased Restrictions of Access

Opponents of abortion did not give up in the wake of *Roe*.[78] A constant onslaught of unnecessary regulations to the procedure followed *Roe* and continue to this day.[79] The United States Supreme Court upheld *Planned Parenthood v. Casey*[80]—the landmark 1992 case creating the "undue burden" standard for state restrictions on abortion—as recently as 2016.[81] Yet, its enforcement has been challenged by changes to the composition of the current Supreme

74. *See* Cynthia Soohoo, *Hyde-Care for All: The Expansion of Abortion-Funding Restrictions Under Health Care Reform*, 15 CUNY L. REV. 391, 391–92 (2012).
75. *See* Andrew S. Murphy, *A Survey of State Fetal Homicide Laws and Their Potential Applicability to Pregnant Women Who Harm Their Own Fetuses*, 89 IND. L.J. 847, 860 (2014); *see* Paltrow & Flavin, *supra* note 19, at 314, 317; Proehl, *supra* note 18, at 668–69; *see* Lynn M. Paltrow, *Roe v Wade and the New Jane Crow: Reproductive Rights in the Age of Mass Incarceration*, 103 AM. J. PUB. HEALTH 17, 17–18 (2013).
76. *See* Soohoo, *supra* note 74, at 398.
77. *See id.*
78. *See infra* Part II.A.
79. *See* Soohoo, *supra* note 74, at 418–20; *see also* Paula Abrams, *Abortion Stigma: The Legacy of Casey*, 35 WOMEN'S RTS. L. REP. 299, 302 (2014) ("More than 755 restrictions on abortion have been enacted since *Casey* issued in 1992. . . . Waiting periods, mandated ultrasounds, prohibitions on late-term abortions, fetal pain and personhood laws, and onerous informed consent requirements typically convey a message of moral disapproval of abortion.").
80. 505 U.S. 833, 874 (1992).
81. Whole Women's Health v. Hellerstedt, 136 S. Ct. 2292, 2309–10 (2016).

Court to a conservative and presumably anti-abortion majority.[82] The 2019 state legislative session included a wave of unprecedented abortion bans in twenty-two Midwestern and Southern states, including a handful that explicitly or effectively outlaw abortion in most circumstances and sought to criminalize pregnant people who seek abortions, abortion providers, and those that assist others in accessing abortion.[83] For example, Louisiana persisted in fighting in federal courts to maintain a law almost identical to a law overturned in *Whole Women's Health,* which required providers to have admitting privileges at local hospitals within thirty miles of their

82. Adam Liptak, *Barrett's Record: A Conservative Who Would Push the Supreme Court to the Right*, N.Y. TIMES (Oct. 15, 2020), https://www.nytimes.com/article/amy-barrett-views-issues.html [https://perma.cc/WZL8-KUV2] ("In a 2013 law review article, [Justice Barrett] examined the role of the doctrine of stare decisis, which is Latin for 'to stand by things decided' and is shorthand for respect for precedent. The doctrine is, Judge Barrett wrote, 'not a hard-and-fast rule in the court's constitutional cases,' and she added that its power is diminished when the case under review is unpopular. 'The public response to controversial cases like Roe,' she wrote, 'reflects public rejection of the proposition that stare decisis can declare a permanent victor in a divisive constitutional struggle.'"); Alexander Bolton, *Democrats Build Abortion Case Against Kavanaugh*, THE HILL (July 10, 2018, 1:22 PM), https://thehill.com/homenews/senate/396317-democrats-build-abortion-case-against-kavanaugh [https://perma.cc/T4W7-NMYF] ("Senate Democrats are pointing to two key decisions that Supreme Court nominee Brett Kavanaugh was involved in to argue he would likely vote to overturn Roe v. Wade, the landmark case that established a woman's right to an abortion.").

83. *See* Sabrina Tavernise & Adeel Hassan, *Missouri Lawmakers Pass Bill Criminalizing Abortion at About 8 of Weeks Pregnancy*, N.Y. TIMES (May 17, 2019), https://www.nytimes.com/2019/05/17/us/missouri-abortion-law.html [https://perma.cc/VZ3U-26NG] ("Under the Missouri law, doctors who perform abortions would be prosecuted and could be sentenced to prison for anywhere between five and 15 years. Women who seek abortions will not be prosecuted."); Amanda Klasing, *Alabama's Abortion Ban Is a Dark Day for Women*, HUM. RTS. WATCH (May 15, 2019, 1:45 PM), https://www.hrw.org/news/2019/05/15/alabamas-abortion-ban-dark-day-women [https://perma.cc/2MN8-WWQX] ("Should that happen, women in Alabama could face jail for having – or even trying to have – an abortion. And other states would surely follow Alabama's lead – some already have similar laws on the books or being considered."); Dartunorro Clark, *Anti-Abortion Bills Mount as GOP-Led States Angle for Supreme Court Fight Over* Roe v. Wade, NBC NEWS (May 12, 2019, 1:58 PM), https://www.nbcnews.com/politics/politics-news/anti-abortion-bills-mount-gop-led-states-angle-supreme-court-n1004366 [https://perma.cc/L4NS-76TE] ("The Georgia bill, she said, signed into law by Republican Gov. Brian Kemp last week, essentially grants personhood to a fetus and, under certain circumstances, could criminalize women who have a miscarriage."); Annalisa Merelli & Ana Campoy, *These Are All the States that Have Adopted Anti-Abortion Laws So Far in 2019*, QUARTZ (May 30, 2019), https://qz.com/1627412/these-are-all-the-states-with-anti-abortion-laws-signed-in-2019/ [https://perma.cc/3LWV-F6QY]; Nash et al., *supra* note 13.

abortion facility.[84] In 2019, the Supreme Court granted certiorari in the case of *June Medical Services, LLC v. Russo*, which was argued before the Supreme Court in March 2020 and decided in June 2020.[85] Many experts feared that the Court would issue a decision that returns decision-making powers regarding the legality of certain abortion practices to state legislatures, thereby turning back the legal rights of pregnant people to pre-1973 regimes in several states that have already passed bans in anticipation of the fall of *Roe*.[86] Although the new abortion bans are likely unconstitutional under *Roe*, if the question is turned back to the states, then pregnant people, abortion providers, and those who assist them will surely see state-sanctioned criminalization in "ban states" and attempts by some prosecutors to bring criminal charges against pregnant people who abort their pregnancies or engage in behavior deemed to threaten a fetus.[87] What we know from U.S. history, as well as present trends, is that those most likely to be criminalized for pregnancy outcomes

84. *See June Medical Services LLC v. Gee Backgrounder*, CTR. FOR REPROD. RTS. (Sept. 17, 2019), https://reproductiverights.org/sites/default/files/2019-09/June%20Medical%20Services%20Backgrounder_September%202019%20%28002%29.pdf [https://perma.cc/KE7H-M58L].

85. *June Medical Services LLC v. Russo*, SCOTUSBLOG, https://www.scotusblog.com/case-files/cases/june-medical-services-llc-v-russo/ [https://perma.cc/5M2S-HJ3L] (last visited Nov. 3, 2020).

86. Joanna L. Grossman, *Women Are (Allegedly) People, Too*, 114 NW. UNIV. L. REV. ONLINE 149, 153–54 (2019) ("Today, constitutional abortion rights hang by a thread, as newly appointed Justices Neil Gorsuch and Brett Kavanaugh portend a stark rightward shift. This has created opportunities for states to restrict abortion—multiple states have passed near or total bans in the last few months in the hopes of bringing about a post-*Roe* world."); Elizabeth Dias et al., *'This is a Wave': Inside the Network of Anti-Abortion Activists Winning Across the Country*, N.Y. TIMES (May 18, 2019), https://www.nytimes.com/2019/05/18/us/anti-abortion-laws.html [https://perma.cc/RWG2-GBEV]. Further, the retirement of Justice Kennedy and replacement of Justice Ruth Bader Ginsburg by Amy Coney Barrett serves only to bolster the validity of such fears. Adam Liptak, *Barrett's Record: A Conservative Who Would Push the Supreme Court to the Right*, N.Y. TIMES (Oct. 15, 2020), https://www.nytimes.com/article/amy-barrett-views-issues.html [https://perma.cc/UQ5P-RCJV]; Josh Gerstein, *How Amy Coney Barrett Might Rule*, POLITICO (Sept. 26, 2020, 7:12 PM), https://www.politico.com/news/2020/09/26/how-amy-coney-barrett-might-rule-422055 [https://perma.cc/R74N-KPU8] (discussing retirement of Justice Kennedy).

87. *See* Dias et al., *supra* note 86; *see, e.g.*, Sarah Mervosh, *Alabama Woman Who Was Shot While Pregnant is Charged in Fetus's Death*, N.Y. TIMES (June 27, 2019), https://www.nytimes.com/2019/06/27/us/pregnant-woman-shot-marshae-jones.html [https://perma.cc/9YU3-S85U].

are people of color, immigrants, low-income individuals, and those with any combination of these characteristics.[88]

Much like the period in the mid-to-late 1800s—when abortion became regulated, criminalized and moved entirely into the realm of mostly male physicians—the current political environment is characterized by heightened levels of xenophobia and a misogynistic preoccupation with preserving white-male privilege.[89] Reproductive rights advocates have responded with a number of creative strategies to meet a potential future when abortion is either outlawed or more restricted; prominent among these strategies is a push to make medication abortion more accessible and to increase access to providers across state lines.[90] Patients access these alternative methods online, through search engines and online information groups.[91] But in a post-*Roe* world, accessing even medicated abortion or self-inducing a termination of pregnancy through any means will still be illegal for people in those states that have

88. Renee B. Sherman, *Recent Abortion Bans Will Impact Poor People and People of Color Most*, VOX (May 18, 2019), https://www.vox.com/first-person/2019/5/18/18630514/missouri-alabama-abortion-ban-2019-racism [https://perma.cc/7V29-7JVM]; Khiara M. Bridges, *Race, Pregnancy, and the Opioid Epidemic: White Privilege and the Criminalization of Opioid Use During Pregnancy*, 133 HARV. L. REV. 770, 815, 820–22 (2020) (analyzing criminalization of poor and white pregnant women despite their white privilege). "[It] is *because* they are racially privileged that they have been subjected to excessive, abusive state power. This is to say that white privilege is present and operating even when white people experience bad outcomes. In many cases, those poor outcomes are direct consequences of white privilege." *Id.* at 776.

89. Jamil Smith, *The Harm Done for White Men*, ROLLING STONE (May 17, 2019, 5:36 PM), https://www.rollingstone.com/politics/politics-features/white-patriarchy-abortion-ban-law-837026 [https://perma.cc/DXY7-TPAX] ("In my native Ohio, a child who is raped might not even know she is pregnant before she runs out of time to abort her rapist's fetus. Missouri sent its eight-week restriction to its eager Republican governor for signature on Friday. And Alabama's law, arguably the most barbaric of them all, criminalizes the procedure from the moment of conception and carries a prison sentence for doctors of up to 99 years. That is a much longer bid than the maximum any rapist in the state could get, all while his victim is forced to bear his child. Each law, in its own way, subjugates women and girls—and since white women statistically have greater access to the procedure, signals a specific attack on women of color. This is a particular issue in Georgia, where noted vote suppressor Brian Kemp is governor. Under the law scheduled to go into effect on January 1st, women who self-terminate their pregnancies can be imprisoned for life or executed, thereby accomplishing two goals: subduing them for their gender, and taking away their ballot. (Men who impregnated them, per the law, suffer no consequence.)").

90. *See Medication Abortion*, GUTTMACHER INST. (Nov. 2019), https://www.guttmacher.org/evidence-you-can-use/medication-abortion [https://perma.cc/TWK2-JECD].

91. *Id.*

outlawed it.[92] This creates the possibility that those who induce or assist a woman with an abortion will be criminalized, with the main tool of investigation being people's web searches and other digital trails.[93] This means that those providing health services and defense lawyers will need to develop new understandings of how the use of technology can expose people to arrest and prosecution.[94]

B. Rise of Self-Induced Abortions

As a result of increasingly restricted access to abortions in clinical settings, people seeking to terminate pregnancies and their advocates have evolved their means of access.[95] Practitioners and patients in the reproductive health care field increasingly rely on abortion pills (commonly referred to as "medication abortion"), which creates new opportunities for access to abortion but also new vulnerabilities for providers and patients.[96] New research by the Guttmacher Institute released in September 2019 found that while abortions performed in clinics have declined since 2014, medication abortion was used by "[a]n estimated 60 percent of women who were early enough in pregnancy [to] [choose] to use abortion pills in 2017 . . . and the pills accounted for 39 percent of all abortions that year. Nearly a third of clinics in 2017 offered only medication abortion."[97] Medication abortions have increased 25% in nonhospital facilities since 2014.[98] The recent availability of medications online, the simplicity of their administration, and the rise of new websites instructing women how

92. *See, e.g.*, Phillips, *supra* note 3.

93. *See supra* note 3 and accompanying text; *see infra* notes 170, 186 and accompanying text.

94. *See, e.g.*, *Our Data Bodies Project*, OUR DATA BODIES, https://www.odbproject.org/wp-content/uploads/2016/12/Appendix-C-Factsheet-r1.pdf [https://perma.cc/95BH-CSEK] (last visited Nov. 4, 2020).

95. *See Medication Abortion*, *supra* note 90.

96. *See id.*; Sherman, *supra* note 88 ("Unfortunately, the 'future' of criminalized abortion is already here. Despite medication abortion pills, for example, being safe enough to self-administer without a provider present, most states do not allow a person to self-manage their own abortion. Should we elect to self-managing our abortions, we are considered the provider and will be prosecuted as such. The risk is not in safety: it's in legality.").

97. Pam Belluck, *America's Abortion Rate Has Dropped to Its Lowest Ever*, N.Y. TIMES, https://www.nytimes.com/2019/09/18/health/abortion-rate-dropped.html [https://perma.cc/NUP9-UGDA] (Sept. 20, 2019) (citing RACHEL K. JONES ET AL., ABORTION INCIDENCE AND SERVICE AVAILABILITY IN THE UNITED STATES, 2017 (2019), https://www.guttmacher.org/sites/default/files/report_pdf/abortion-incidence-service-availability-us-2017.pdf [https://perma.cc/8H78-FZVV]).

98. JONES ET AL., *supra* note 13, at 8, 20 tabl.6.

to self-induce abortions make it inevitable that medication abortions will only increase in the future, especially as clinics continue to close and new restrictions on abortion access are legislated.[99] The Guttmacher report also documents a parallel increase in self-managed abortions, up from 12% since 2014 to 18% in 2017, with the highest reported numbers coming from non-hospitals in the Southern and Western regions of the United States.[100]

III. THE TECH-ASSISTED FUTURE CRIMINALIZATION OF PREGNANT PEOPLE AND ABORTION PROVIDERS

A. Tech-Assisted Future Criminalization of People.

For all the reasons discussed in Part II—lack of access, privacy, privilege, money, and mobility—pregnant people are now more likely to self-manage their abortions rather than visit a medical facility.[101] Like many Americans seeking medical advice, the first obvious step many pregnant people will take to self-manage their abortion will be what they may assume to be a solitary consultation with their personal digital device.[102] Whether this leads them to an online medical or commercial provider of abortion pills, or a network of underground abortion doulas, this initial research that lends a false sense of privacy may leave a detailed data trail for those whose devices later become evidence in an investigation.[103]

In addition to online search histories, other types of digital evidence can also be culled to support a prosecution, including location-tracking data, website navigation histories, purchasing history, social media activity, wearable device data, data entered into apps, and home devices connected to the internet.[104]

1. Most Americans seek medical advice online at increasing rates.

Nearly twenty years ago, the Pew Internet & American Life Project released a study documenting that already "80 percent of Internet users, or about 93 million Americans, have searched for at least one

99. *See id.* at 1; Megan K. Donovan, *Self-Managed Medication Abortion: Expanding the Available Options for U.S. Abortion Care*, 21 GUTTMACHER POL'Y REV. 41, 41 (2018).
100. JONES ET AL., *supra* note 13, at 8.
101. *See supra* Part II.
102. *Many Young Women in the United States Turn to Google for Information on Self-Abortion*, GUTTMACHER INST. (Feb. 26, 2018), https://www.guttmacher.org/news-release/2018/many-young-women-united-states-turn-google-information-self-abortion [https://perma.cc/9EGJ-TJQV].
103. *See infra* Section III.A.3.
104. *See infra* Section III.A.6.

of 16 major health topics online."[105] Since 2003, the number of Americans searching for major health topics online has increased as web-based medical information is replacing shortages in doctors, medical facilities, and hospitals, which are all drastically decreasing in rural areas due to lower Medicaid funding.[106] This still leaves gaps in services, for example, in rural areas, accessing the internet may still be through a phone connection rather than broadband.[107] Many in the medical community embrace the development of online medical care, emphasizing that while online, doctors can diagnose and treat a large range of issues.[108] Additionally, "[p]rescriptions may be transmitted to pharmacies and patients never need to go to an overcrowded, germ riddled doctor's office for evaluation and a prescription."[109] The same satisfaction is reported among patients, who prefer the online experience because of the "convenience and decreased costs. Some patients felt more comfortable with video visits than office visits and expressed a preference for receiving future serious news via video visit, because they could be in their own supportive environment."[110] While some patients reported concerns about privacy, it was mainly in the context of whether their

105. Jane Weaver, *More People Search for Health Online*, NBC NEWS (July 16, 2003, 4:15 AM), www.nbcnews.com/id/3077086/t/more-people-search-health-online#.X0vhMchKhPZ [https://perma.cc/FX2E-K5BK].

106. *The State of Online Medical Care in 2020*, ONLINE DR., https://onlinemedicalcare.org/state-of-online-medical-services/ [https://perma.cc/MX3V-KH2P] (last visited Nov. 3, 2020) ("[T]he U.S. will experience a shortage of over 100,000 physicians by 2030 . . . ."); THE CHARTIS GRP., THE RURAL HEALTH SAFETY NET UNDER PRESSURE: RURAL HOSPITAL VULNERABILITY 2, 4 (Feb. 2020), https://www.ivantageindex.com/wp-content/uploads/2020/02/CCRH_Vulnerability-Research_FiNAL-02.14.20.pdf [https://perma.cc/EKZ3-EYQC] ("[T]he [hospital] closure crisis has affected rural hospitals located in non-Medicaid expansion states much more so than in states that have expanded Medicaid.").

107. *Eighth Broadband Progress Report*, FED. COMMC'NS COMM'N, https://www.fcc.gov/reports-research/reports/broadband-progress-reports/eighth-broadband-progress-report [https://perma.cc/85FE-EW73] (last visited Nov. 3, 2020) ("[A]pproximately 19 million Americans—6 percent of the population—still lack access to fixed broadband service at threshold speeds. In rural areas, nearly one-fourth of the population—14.5 million people—lack access to this service. In tribal areas, nearly one-third of the population lacks access. Even in areas where broadband is available, approximately 100 million Americans still do not subscribe.").

108. *The State of Online Medical Care in 2020*, *supra* note 106.

109. *Id.*

110. Rhea E. Powell et al., *Patient Perceptions of Telehealth Primary Care Video Visits*, 15 ANNALS FAM. MED. 225, 225 (2017).

coworkers could overhear, and not about what digital trails their engagement was leaving.[111]

2. Pregnant people are also seeking medical advice online at increasing rates.

Pregnant people seeking information about their reproductive health are going online for the same reasons.[112] Like everyone else seeking information online, they prefer the online experience because of the decreased costs, the appeal of not traveling, and having the ability to manage their health in what feels like a private manner.[113] While the online environment gives the seeker of medical information a feeling of privacy, internet use is actually easily surveilled.[114] Every mouse or finger hover, click, keystroke, pause, and purchase is recorded and tracked.[115] This is especially true for pregnant people.[116] Research by advertising companies has taught them that major life events, like pregnancy, can trigger new spending habits that companies want to capitalize on.[117] "Parents-to-be are incredibly valuable customers, guaranteed to drop lots of money for 18 years or more, so companies go to great lengths to identify them and to snag them as customers."[118] In other words, the profile of a person who may be pregnant or trying to become pregnant is already defined by data collection firms who sell those profiles to

111. *Id.* at 227 ("While they noted the advantage of not missing work, those without private offices struggled to find space where coworkers would not overhear. One person reported that the inability to achieve privacy at work impaired their ability to have a proper exam. A few participants suggested potential workplace privacy solutions including use of headphones and reserving office space for the visit.")

112. Marie Solis, *3 Women on What It's like to Give Yourself an Abortion*, VICE (Feb. 24, 2020, 8:00 AM), https://www.vice.com/en_us/article/epg5xm/give-yourself-an-abortion-with-pills-bought-online-aid-access [https://perma.cc/5L7A-4UGB].

113. *Id.*

114. *See* Jacob Kastrenakes, *Congress Just Cleared the Way for Internet Providers to Sell Your Web Browsing History*, THE VERGE (Mar. 28, 2017, 5:57 PM), https://www.theverge.com/2017/3/28/15080436/us-house-votes-to-let-isps-share-web-browsing-history [https://perma.cc/59MD-7EJ9].

115. *See id.*

116. Kelly Bourdet, *Target Knows You're Pregnant*, VICE (Feb. 18, 2012, 5:26 PM), https://www.vice.com/en_us/article/qkkepv/target-knows-you-re-pregnant [https://perma.cc/B4H5-6TEP].

117. *Id.*

118. Kashmir Hill, *You Can Hide Your Pregnancy Online, but You'll Feel like a Criminal*, FORBES (Apr. 29, 2014, 8:30 AM), https://www.forbes.com/sites/kashmirhill/2014/04/29/you-can-hide-your-pregnancy-online-but-youll-feel-like-a-criminal/#26ea761921f3 [https://perma.cc/Y8J7-VSE9].

advertisers.[119] They have refined this profile so well for the pregnant demographic that, in at least one situation, advertisers were aware of a pregnancy before the pregnant girl knew, or at least before she informed her father.[120] In 2012, a father stormed into a large retail store upset that it was mailing advertisements for baby items to his teenage daughter, only to find out one week later that she was indeed pregnant.[121]

In response to this news story, a Princeton sociology professor, Janet Vertesi, attempted to hide her pregnancy from the internet.[122] She and her husband bought gift cards, used cash, and did not mention the pregnancy in social media, emails or texts.[123] She relied on her friends and family also following strict rules about not mentioning her pregnancy in online communications.[124] She successfully went through pregnancy without the usual bombardment of baby-related ads targeted at her, but did not recommend this approach to others: "[o]pting out makes you look like a criminal . . . . [i]t's incredibly inconvenient. It isn't sustainable . . . ."[125] For a person like Professor Vertesi, who is pregnant and wants to hide their status from the internet, even taking basic protective measures to avoid digital tracking can prove problematic.[126] Some of the steps Professor Vertesi was required to take to avoid digital tracking raised red flags.[127] For example, "her husband had to get over $500 in gift cards at a Rite Aid, where he noticed a warning that the Rite Aid might limit prepaid card purchases and was required to 'report excessive transactions to the authorities.'"[128] While her experiment did not result in actual criminal consequences for her or her husband, it easily could have for a person with different social status or skin color.[129]

119. Lois Beckett, *Everything We Know About What Data Brokers Know About You*, PROPUBLICA (June 13, 2014, 1:59 PM), https://www.propublica.org/article/everything-we-know-about-what-data-brokers-know-about-you [https://perma.cc/HLK6-2Y77].
120. Bourdet, *supra* note 116.
121. *Id.*
122. Hill, *supra* note 118.
123. *Id.*
124. *Id.*
125. *Id.*
126. *Id.*
127. *Id.*
128. *Id.*
129. *See infra* Part III.A.3.

People seeking to self-manage their abortions online commonly search for and purchase abortion pills.[130] Abortion pills are the potential "Holy Grail"[131] of reproductive health because they are portable, simple to self-administer, and safe.[132] With the ability to purchase them online, abortion pills have all but replaced traditional abortion procedures in medical settings.[133] Responding to Guttmacher Institute's 2019 findings of decreased abortions in the United States, the New York Times pointed to abortion pills purchased online in an article titled *Why America's Abortion Rate Might Be Higher Than It Appears.*[134] It reported that Aid Access, an online abortion-pill medical provider,[135] "reported 21,000 requests for medications for self-induced abortions last year, in its first year in the country. Plan C, which provides information about self-managed medication abortions, reports about 40,000 online visitors a month."[136] From January 2015 through January 2020, consistent searches for "abortion pills" were made in thirty-nine states, most frequently in Mississippi, Louisiana, Georgia, Alabama, and Texas.[137] Of course, most of these states have seen new restrictions on abortion introduced in the past few years.[138]

---

130. *See* Beverly Winikoff, *Will a New Kind of Pill Be the Holy Grail We Seek?*, CONSCIENCE (Sept. 20, 2019), https://consciencemag.org/2019/09/20/will-a-new-kind-of-pill-be-the-holy-grail-we-seek/ [https://perma.cc/B5XB-JAY2].

131. *Id.*

132. The SIA Legal Team, *supra* note 48; Aiken et al., *supra* note 49 (finding that "[s]elf sourced medical abortion using online telemedicine can be highly effective, and outcomes compare favourably with in clinic protocols"); Belluz, *supra* note 49; WORLD HEALTH ORG., *supra* note 49, at 46; Winikoff et al., *supra* note 49 ("The medical regimen had more side effects, particularly bleeding, than did surgical abortion but very few serious side effects. Failure rates for medical abortion, although low, exceeded those for surgical abortion: 8.6% versus 0.4% (China), 16.0% versus 4.0% (Cuba), and 5.2% versus 0% (India). Nearly half of failures among medical clients were not true drug failures, however, but surgical interventions not medically necessary (acceptability failures or misdiagnoses). Women were satisfied with either method, but more preferred medical abortion.").

133. *See* Claire Cain Miller & Margot Sanger-Katz, *Why America's Abortion Rate Might Be Higher Than It Appears*, N.Y. TIMES (Sept. 20, 2019), https://www.nytimes.com/2019/09/20/upshot/abortion-pills-rising-use.html [https://perma.cc/JN9L-RV9H]; Katie Kindelan, *'Self-induced Abortion' Searches on Google Reflect a Dark Reality for Many Women*, ABC NEWS (July 9, 2018, 4:27 AM), https://abcnews.go.com/GMA/News/induced-abortion-searches-google-reflect-dark-realitywomen/story?id5623222 [https://perma.cc/KX2Y-KYW6].

134. *See generally* Miller & Sanger-Katz, *supra* note 133.

135. *See infra* Part III.B.

136. Miller & Sanger-Katz, *supra* note 133.

137. *"Abortion Pills"*, GOOGLE TRENDS, https://trends.google.com/trends/explore?date=today%205y&geo=US&q=abortion%20pills [https://perma.cc/NS6T-HJQA] (last visited

A report published in Contraception Magazine confirmed that most of these websites are delivering real pills.[139] The researchers "searched the internet to identify a convenience sample of websites that sold mifepristone and misoprostol to purchasers in the United States and attempted to order these products."[140] They identified the prices, shipping times and additional details regarding the ordering process, and finally tested the samples in labs.[141] In their conclusion the researchers stated as follows:

> Our study found no evidence that, at the time of the study, mifepristone and misoprostol products sold online were dangerous or ineffective. We encourage reproductive health providers, advocates and policy makers to think creatively about how the internet might be useful for enhancing access

---

Nov. 9, 2020). Google Trends documents the frequency with which people have searched for specific terms online with chronologies, geographic breakdown in the United States, related topics, and related queries. *See, e.g.*, *id.*

> Google Trends normalizes search data to make comparisons between terms easier. Search results are normalized to the time and location of a query by the following process:
>
> - Each data point is divided by the total searches of the geography and time range it represents to compare relative popularity. Otherwise, places with the most search volume would always be ranked highest.
> - The resulting numbers are then scaled on a range of 0 to 100 based on a topic's proportion to all searches on all topics.
> - Different regions that show the same search interest for a term don't always have the same total search volumes.

FAQ About Google Trends Data, GOOGLE: TRENDS HELP, https://support.google.com/trends/answer/4365533?hl=en [https://perma.cc/6JQS-GAFE] (last visited Nov. 4, 2020).

138. *See* Elizabeth Nash et al., *supra* note 13. To clarify, there are two articles by Elizabeth Nash cited at note 13. This note cites the Nash source titled "*State Policy Trends 2019: A Wave of Abortion Bans, but Some States Are Fighting Back*."
139. Chloe Murtagh et al., *Exploring the Feasibility of Obtaining Mifepristone and Misoprostol from the Internet*, 97 CONTRACEPTION 287, 287 (2018).
140. *Id.*
141. *Id.* at 288.

> to safe and effective abortion in the United States and other similarly disadvantaged settings.[142]

This increased reliance on web-based services—from the online search engine to the website for abortion pill vendors to the cashless purchase of pills online—forces a pregnant person to engage with a system that actively collects, stores, and sells their online activity data.[143]

This exposure is not unique to pregnant people, but the risk of exposure carries more consequences for them if their digital devices become evidence in a case against them or an abortion pill provider.[144] Anti-abortion activists and lawmakers are already on the offensive against this trend; for example, Texas anti-choice activists are advocating for a bill that would make it a felony to mail abortion pills to someone in Texas, allowing the State to prosecute and demand extradition of the accused person to Texas.[145]

---

142. *Id.* at 291.

143. *See* Stuart A. Thompson & Charlie Warzel, *Twelve Million Phones, One Dataset, Zero Privacy*, N.Y. TIMES (Dec. 19, 2019), https://www.nytimes.com/interactive/2019/12/19/opinion/location-tracking-cell-phone.html [https://perma.cc/5QCN-4MVA] ("The data reviewed by the Times . . . didn't come from a telecom or giant tech company, nor did it come from a governmental surveillance operation. It originated from a location data company, one of dozens quietly collecting precise movements using software slipped onto mobile phone apps. You've probably never heard of most of the companies — and yet to anyone who has access to this data, your life is an open book. They can see the places you go every moment of the day, whom you meet with or spend the night with, where you pray, whether you visit a methadone clinic, a psychiatrist's office or a massage parlor."). COVID-19 has escalated that reliance, prompting calls from advocates and the medical profession to the Food and Drug Administration (FDA) to loosen the current requirement that medication abortions be prescribed with a clinical exam. *See, e.g.*, *The Coronavirus Crisis Must Be a Wake-Up Call to Demand Reproductive Self-Determination for All*, IF/WHEN/HOW, https://www.ifwhenhow.org/wp-content/uploads/2020/04/20_04_02_Policy_Platform_COVID19_FINAL.pdf [https://perma.cc/4Z8B-PAFA] (last visited Nov. 5, 2020); *see also* Patrick Adams, *Amid Covid-19, a Call for M.D.s to Mail the Abortion Pill*, N.Y. TIMES (May 12, 2020), https://www.nytimes.com/2020/05/12/opinion/covid-abortion-pill.html [https://perma.cc/EL3B-FWDV].

144. *See infra* Sections III.A.3–.7.

145. María Méndez, *As More People Search for Abortion Pills Online, Texas Opponents Push to Restrict Access*, DALL. MORNING NEWS (Dec. 2, 2019), https://www.dallasnews.com/news/politics/2019/12/02/as-more-people-search-for-abortion-pills-online-texas-opponents-push-to-restrict-access/ [https://perma.cc/R7UH-MZZ2].

3. Searches of digital devices by state agencies is an increasingly common form of surveillance, especially of Black individuals and other people of color dependent on state resources.

The risk of going online for information related to terminating a pregnancy may feel remote, and for some pregnant people, it is.[146] For the majority of people searching for health-related information online, whether anyone will ever review their search or purchasing history is, at best, a remote possibility.[147] But internet access has become increasingly affordable to a larger population.[148] In 2019, the Pew Research Center on the Internet and Technology reported in 2019 that those who are "Smartphone Dependent" now commonly includes "younger adults, non-whites and lower-income Americans," and that the majority of Americans from a wide-range of demographic backgrounds own a smartphone.[149]

Young people of color, including girls and women from low-income communities, are surveilled, searched and seized by multiple state authorities at disproportionately higher rates than their white peers, making it more likely that their digital devices will be as well.[150] Black communities specifically have suffered more intrusive levels of surveillance dating back to slavery.[151] "Plantation ledger books served as proto-biometric databases, recording the slaves as

146. *See* BARTON GELLMAN & SAM ADLER-BELL, THE DISPARATE IMPACT OF SURVEILLANCE 5–6 (2017), https://production-tcf.imgix.net/app/uploads/2017/12/03151009/the-disparate-impact-of-surveillance.pdf [https://perma.cc/VWN2-RHZQ].

147. *See id.*

148. *See Internet/Broadband Fact Sheet*, PEW RES. CTR. (June 12, 2019), https://www.pewresearch.org/internet/fact-sheet/internet-broadband/ [https://perma.cc/7N3L-79J9]; LOGAN KOEPKE ET AL., MASS EXTRACTION: THE WIDESPREAD POWER OF U.S. LAW ENFORCEMENT TO SEARCH MOBILE PHONES 4, (2020), https://www.upturn.org/static/reports/2020/mass-extraction/files/Upturn%20-%20Mass%20Extraction.pdf [https://perma.cc/7D2G-XNBC].

149. *See Internet/Broadband Fact Sheet*, *supra* note 148. Following the COVID-19 outbreak, reliance on digital devices for everything from telemedicine to "remote learning" has obviously increased. *U.S. Study Finds COVID-19 Pandemic Transforms Cell Phone Usage*, CISION (May 28, 2020), https://www.prnewswire.com/news-releases/us-study-finds-covid-19-pandemic-transforms-cell-phone-usage-301066502.html [https://perma.cc/D8CN-9FM7].

150. *See supra* note 32 and accompanying text; Melinda D. Anderson, *When School Feels Like Prison*, THE ATLANTIC (Sept. 12, 2016), https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556/ [https://perma.cc/L47L-S9JU].

151. GELLMAN & ALDER-BELL, *supra* note 146.

physical specimens in fine detail. The slave pass, the slave patrol, and the fugitive slave poster—three pillars of information technology in their day—prefigured modern policing, tracking, and photo ID."[152] Control over the physical body during slavery extended to control over Black women's bodies and reproductive health as well.[153]

> [C]hildbearing during slavery was often intrinsically related to an economic system that benefitted white slave owners more so than a matter of personal freedom. Because enslaved women and girls were denied reproductive rights to control their own sexuality, they were unable to determine with whom they engaged in sexual relationships. Women who were considered 'strong' were sold as breeders and routinely sexually assaulted to birth more children into slavery. Some enslaved females attempted to avoid being sexually exploited for these purposes and aborted their pregnancies as an act of resistance.[154]

Civil and criminal justice actors—whether police, social workers or public health care workers—can gain access to one's digital devices through a variety of tools.[155] Most commonly, people share their devices upon request by a social worker, police officer, counselor, or nurse during a questioning that may range from feeling like a casual conversation to a coercive interrogation.[156] Some public welfare

---

152. *Id.*

153. DOROTHY ROBERTS, KILLING THE BLACK BODY: RACE, REPRODUCTION, AND THE MEANING OF LIBERTY, 27–28 (1998) ("The law reinforced the sexual exploitation of slave women in two ways: it deemed any child who resulted from the rape to be a slave and it failed to recognize the rape of a slave woman as a crime.").

154. Cynthia Prather et al., *Racism, African American Women, and Their Sexual and Reproductive Health: A Review of Historical and Contemporary Evidence and Implications for Health Equity*, 2 HEALTH EQUITY 249, 251 (2018) (footnotes omitted).

155. *See* Danielle Keats Citron, Comment, *A Poor Mother's Right to Privacy: A Review*, 98 B.U. L. REV. 1139, 1144 (2018) ("When pregnant women seek government assistance for medical care, the State demands a dizzying array of personal information. In addition to the expected health exams to determine pregnant women's physical health, state Medicaid rules require assessments of their 'nutritional status, health education status, and psychosocial status.' Data is collected about poor pregnant women's 'formal education and reading level,' 'religious and cultural influences,' 'history of previous pregnancies,' 'general emotional status and history,' 'wanted or unwanted pregnancy,' 'personal adjustment to pregnancy,' 'substance use and abuse,' 'housing/household,' and 'education/employment.'") (footnotes omitted); *id.* at 1162.

156. *See id.* at 1142 (explaining most vulnerable members of society heavily surveilled and must surrender information to receive public benefit programs); *see also* KOEPKE ET AL., *supra* note 148, at 46–47.

agencies have the ability to track a recipient's purchasing data tracked by the Electronic Benefit Transfer (EBT) cards they provide for basic necessities.[157] Some countries, states, and cities around the world have even expanded this to include biometric data collection as a condition of state welfare programs.[158] Federal law enforcement agencies increasingly request warrants and subpoenas for cell phone and computer data during the course of an investigation before charging the accused with the relevant crime.[159] After a criminal prosecution has been initiated, a prosecutor may also ask the accused to sign a waiver allowing them to access their phone or request a warrant from the court.[160]

---

157. *See* Mario Moretto, *LePage Releases EBT Data Showing Transactions at Strip Clubs, Bars, Smoke Shops*, BANGOR DAILY NEWS (Jan. 7, 2014), https://bangordaily news.com/2014/01/07/politics/lepage-releases-ebt-data-showing-transactions-at-strip-clubs-bars-smoke-shops/ [https://perma.cc/UQQ8-RS2R].

158. *See* Frank Hersey, *2019: A Critical Year for Biometrics and Digital ID in the Global South*, BIOMETRIC UPDATE (Dec. 23, 2019), https://www.biometricupdate.com/201912 /2019-a-critical-year-for-biometrics-and-digital-id-in-the-global-south [https://perma. cc/83R2-PA9B] (illustrating how various governments are implementing universal biometric ID schemes and how healthcare services are starting to incorporate these schemes).

159. *See* David Kravets, *We Don't Need No Stinking Warrant: The Disturbing, Unchecked Rise of the Administrative Subpoena*, WIRED (Aug. 28, 2012, 6:00 AM), https://www.wired.com/2012/08/administrative-subpoenas/ [https://perma.cc/J2YE-HCQ2].

> With a federal official's signature, banks, hospitals, bookstores, telecommunications companies and even utilities and internet service providers – virtually all businesses – are required to hand over sensitive data on individuals or corporations, as long as a government agent declares the information is relevant to an investigation. Via a wide range of laws, Congress has authorized the government to bypass the Fourth Amendment – the constitutional guard against unreasonable searches and seizures that requires a probable-cause warrant signed by a judge. In fact, there are roughly 335 federal statutes on the books . . . passed by Congress giving dozens upon dozens of federal agencies the power of the administrative subpoena, according to interviews and government reports.

Id.

160. *See* Dana Littlefield, *Does Digital Privacy Extend to Criminals on Probation?*, SAN DIEGO UNION TRIB. (Jan. 15, 2016, 4:35 PM), https://www.sandiegouniontribune.com /sdut-court-waiver-cellphone-passwords-search-privacy-2016jan15-story.html [https: //perma.cc/9Y9Q-BAF2] (illustrating example of criminal court defendants asked to sign waiver to grant prosecution access to cell phone device and password); *see*

In the modern context, racial disparities in state surveillance programs are usually associated with violations of policing powers, such as the New York City Police Department's (NYPD) extensive stop and frisk program in New York City, which subjected hundreds of thousands of black and brown New Yorkers to unconstitutional violations of their body.[161] People were not just subjected to stops with questioning, they were subject to "being forcibly stripped to their underclothes in public, inappropriate touching, physical violence and threats, extortion of sex, sexual harassment and other humiliating and degrading treatment."[162] A federal court ruling forced the NYPD to drastically reduce its use of stop and frisk, but it still occurs and is underreported.[163] Street stops can be one of the means through which people's digital devices are searched or confiscated by state law enforcement.[164] For example, some New Yorkers have complained that police have searched or deleted information from their electronic devices during a street stop.[165]

People may or may not additionally share a password with officers, but they may not need to.[166] While some courts have ruled that the Fifth Amendment protection against self-incriminating testimony prohibits government authorities from forcing people to share their passwords to devices containing potentially incriminating

---

generally Riley v. California, 573 U.S. 373, 373 (2014) (holding warrant generally required before police can search a defendant's cell phone).

161. *See* CTR. FOR CONST. RTS., STOP AND FRISK: THE HUMAN IMPACT 3 (Sarah Hogarth ed., 2012).

162. *Id.* at 5.

163. *See* Al Baker, *Street Stops by New York City Police Have Plummeted*, N.Y. TIMES (May 30, 2017), https://www.nytimes.com/2017/05/30/nyregion/nypd-stop-and-frisk.html [https://perma.cc/3CVB-Q76Q].

164. *See Stop, Question and Frisk*, CIVILIAN COMPLAINT REV. BD., https://www1.nyc.gov/site/ccrb/investigations/stop-question-and-frisk.page [https://perma.cc/4MA3-5LF3] (last visited Nov. 5, 2020) (illustrating the varying levels of intrusion possible during a street encounter with an officer, including the examination of data contained in a cell phone).

165. *See What Types of Abuse of Authority Allegations Have The CCRB Received Over Time?*, CIVILIAN COMPLAINT REV. BD. (Aug. 28, 2020), https://www1.nyc.gov/site/ccrb/policy/data-transparency-initiative-allegations.page#abuse_authority [https://perma.cc/JA53-B5Y8] (referring to abuse of authority allegations chart in support of proposition that police have deleted information from civilian's phones during a street stop).

166. *See* Susan W. Brenner, *The Fifth Amendment, Cell Phones and Search Incident: A Response to Password Protected?*, 96 IOWA L. REV. BULL. 78, 83–86 (2011) (illustrating responses available to an arrested individual when asked to provide a password to his phone).

information,[167] the advent of biometric data (fingerprints and facial recognition)[168] as a means of unlocking a phone or other device has strained the definition of "testimony," making those protections—as applied to digital devices—unreliable in some jurisdictions.[169] If people do not voluntarily hand over their devices to police investigators, or if the devices have been separately seized pursuant to a subpoena or a search warrant, some data is still accessible through digital forensics technologies pursuant to a search warrant or a subpoena for the search engine or internet service provider (ISP).[170]

If the device was seized, or if the police took a device with a person's consent, mobile device forensic tools such as Cellebrite machines have the ability to create a copy of a smartphone or other digital device and save it to an external hard drive or USB flash drive.[171] This copy allows an investigator to easily peruse a phone's contents through keyword searches, image searches, social network analyses, and geographic maps, all in a user-friendly presentation.[172] Mobile device forensic tools, used by over 2,000 agencies across the United States—including housing authorities, prisons, public schools, and all sizes of police departments—can pull three types of

167. *See id.* at 86–88; Jesse Coulon, Comment, *Privacy, Screened Out: Analyzing the Threat to Individual Privacy Rights and Fifth Amendment Protections in* State v. Stahl, 59 B.C. L. REV. E. SUPP. 225, 227 (2018) ("Courts have answered this question in a variety of different ways with a range of results, but no court prior to the Florida Second District Court of Appeals in 2016, in *State v. Stahl*, has completely stripped away an individual's Fifth Amendment right to refuse to give law enforcement the password to a personal encrypted device.").

168. *See* Shams, *List of All Fingerprint Scanner Enabled Smartphones*, WEBCUSP (Apr. 24, 2018), https://webcusp.com/list-of-all-fingerprint-scanner-enabled-smartphones/ [https://perma.cc/5UZU-3GZC].

169. *See* Heidi Kuffel & Katelyn Rauh, *"Face ID is Unavailable. Try Again Later" — Can Law Enforcement Force a Suspect to Unlock Their Phone by Face ID or Fingerprint?*, ABA (Feb. 13, 2019), https://www.americanbar.org/groups/business_law/publications/committee_newsletters/cyberspace/2019/201902/fa_1/ [https://perma.cc/3DS2-CN6C]; *see* Opher Shweiki & Youli Lee, *Compelled Use of Biometric Keys to Unlock A Digital Device: Deciphering Recent Legal Developments*, 67 DEP'T JUST. J. FED. L. & PRAC. 23, 23 (2019).

170. *See* U.S. DEP'T OF JUST., DIGITAL EVIDENCE IN THE COURTROOM: A GUIDE FOR LAW ENFORCEMENT AND PROSECUTORS 3 (2007), https://www.ncjrs.gov/pdffiles1/nij/211314.pdf [https://perma.cc/VG5Y-UDLK].

171. Jonathan Adkins, *Cellebrite Mobile Forensics Tool Demonstration*, YOUTUBE (Sept. 9, 2018), https://www.youtube.com/watch?v=5fEYqpJ6Mrw. Other companies that sell mobile device forensic tools include Grayshift, MSAB, Magnet Forensics, and AccessData. KOEPKE ET AL., *supra* note 148, at 11.

172. *See* Adkins, *supra* note 171; *see* KOEPKE ET AL., *supra* note 148, at 10.

information.[173] A logical extraction, most commonly used, pulls text messages, contact information, call logs, music files, app data, pictures, videos, and calendars.[174] File systems and physical extractions pull even more information, including files and hidden files.[175] Physical extractions pull all the deleted data on the phone, in addition to everything pulled by a logical extraction and a file system extraction.[176] Some forensic tools can even pull data off of "the Cloud" through one's mobile device.[177]

Information from a digital device—whether a wearable "watch," phone or tablet—can collect information about an accused's location history, movements, and *mens rea* (criminal intent) during the time period a crime is believed to have occurred.[178] Many criminal prosecutions that would have stalled without digital evidence resulted in convictions either at trial or in plea bargaining because the digital evidence completed the picture of the accused's involvement, state of mind, or intent.[179]

One recent example of digital data comes from the 2018 trial in New York City of Chanel Lewis for murdering a woman named Karina Vetrano.[180] Detectives confiscated Lewis' phone from the top of his dresser during a search of his bedroom.[181] The detective testified at trial that the phone documented web searches for terms such as "arraignment," "After a Crime, the Price of a Second Chance," "Miranda warning," "what happens after a felony conviction?" in addition to the Catholic "Sacrament of Penance" Wikipedia page.[182] These web searches, in combination with two

173. *See* Adkins, *supra* note 171; *see* KOEPKE ET AL., *supra* note 148, at 32.
174. *See* Adkins, *supra* note 171; *see generally* KOEPKE ET AL., *supra* note 148, at 10–31 (providing screenshots of forensic tools illustrating appearance of smartphone analysis to police and prosecutors).
175. *See* Adkins, *supra* note 171.
176. *Id.*
177. *Cellebrite UFED Cloud*, CELLEBRITE, https://www.cellebrite.com/en/ufed-cloud/ [https://perma.cc/2GQV-TPPH] (last visited Nov. 4, 2020); *see* KOEPKE ET AL., *supra* note 148, at 17.
178. *See* GOODISON ET AL., *supra* note 50, at 3, 7.
179. *See, e.g.*, *infra* notes 180–88 and accompanying text.
180. Noah Goldberg & Larry McShane, *Accused Queens Jogger Killer's Cell Phone Offered Glimpse into His Post-killing State of Mind*, N.Y. DAILY NEWS (Nov. 13, 2018, 2:20 PM), https://www.nydailynews.com/new-york/nyc-crime/ny-metro-queens-jogger-trial-20181113-story.html [https://perma.cc/DF39-87ZM].
181. *Id.*
182. *Id.*

photos of Vetrano and one of the crime scene, saved from news articles, were used as evidence of Lewis' criminal intent.[183]

Prosecutors in the trial of Casey Anthony, a young mother accused of killing her toddler daughter, also relied on digital forensics analysis to argue that Anthony used the family computer to search for "chloroform" eighty-four times on the day her daughter was killed, even though it was only once in reality.[184] The investigation of the murder of Christian Aguilar at the University of Florida in 2012 also rested on digital evidence.[185] Without many leads, detectives focused on a friend of Aguilar's, Pedro Bravo, and obtained his digital device.[186] His digital trails revealed a Siri search for "I need to hide my roommate," location information placing Bravo along the same route Aguilar's body had been found, and prolonged use of the "flashlight" app an hour after the disappearance.[187] Primarily based on this digital evidence, Bravo was convicted.[188]

When digital forensics are applied to prosecute a murder case, it is easy to applaud the power of these tools to peek in the "window into the soul."[189] Prosecutors and police do not restrict the use of their digital tools to cases involving serious violent felonies.[190] Across the

183. *See* WKRC, *Accused Killer's Cell Phone Showed Photos of Victim, Searches for Forgiveness*, LOC. 12 (Nov. 14, 2018), https://local12.com/news/nation-world/accused-killers-cell-phone-showed-photos-of-victim-searches-for-penance [https://perma.cc/YZ5Q-S5TN].

184. Lizette Alvarez, *Software Designer Reports Error in Anthony Trial*, N.Y. TIMES (July 18, 2011), https://www.nytimes.com/2011/07/19/us/19casey.html [https://perma.cc/38KP-37SF]. Days after Anthony was acquitted, the developer of the software used to conduct this analysis disputed that finding publicly, clarifying that the browser search for "chloroform" had only happened once (not eighty-four times) and that the prosecutor had withheld that correction from the defense. *Id.* After acquittal, other reports of Anthony's Mozilla browser history claimed finding "foolproof suffocation" or "neck (plus) breaking." C.M. "Mike" Adams, *Digital Forensics: Window into the Soul*, FORENSIC (June 10, 2019), https://www.forensicmag.com/518341-Digital-Forensics-Window-Into-the-Soul/ [https://perma.cc/L33E-DE32].

185. GOODISON ET AL., *supra* note 50, at 2.

186. *Id.*

187. Laura Mandaro, *Murder Suspect's iPhone History Takes Central Role*, USA TODAY, https://www.usatoday.com/story/news/nation-now/2014/08/13/siri-murder-dead-body/14019383/ [https://perma.cc/U5BZ-WX6G] (Aug. 13, 2014, 6:58 PM).

188. *See* Audra D.S. Burch, *Pedro Bravo Found Guilty of First-Degree Murder of Christian Aguilar*, MIA. HERALD (Sept. 12, 2014, 11:53 AM), https://www.miamiherald.com/news/local/community/miami-dade/article1980000.html [https://perma.cc/A8GP-EDUU].

189. *See* Adams, *supra* note 184.

190. *See* Kashmir Hill, *Imagine Being On Trial. With Exonerating Evidence Trapped on Your Phone.*, N.Y. TIMES (Nov. 22, 2019), https://www.nytimes.com/2019/11/22/bus

U.S., police and prosecutors conducted at least 50,000 extractions of digital devices between 2015 and 2019 for a wide range of crimes including graffiti, shoplifting, marijuana possession, car crashes, vandalism, parole violations, public intoxication, prostitution, grand larceny, promoting prostitution, petit larceny, fraud, trafficking, drug possession, unlawful disclosure of an intimate image, unlawful surveillance, and more.[191] The old adage "if you have a hammer, you treat everything like a nail," often repeated by public defenders and prosecutors alike to describe state powers, applies in the digital world as well.[192] If abortion, self-induced abortion, possession of abortion pills, mailing of abortion pills, or assisting an abortion are criminalized across the U.S., there is no reason to believe that prosecutors or police will hesitate to perform forensics analysis on digital devices as part of an investigation into unlawful abortions.[193] In fact, this new opportunity to pierce pregnant people's mindsets may encourage accelerated criminalization and pretextual investigations since it simplifies the evidence gathering and surveillance needed to convict people.[194]

This level of intrusion is also unfair to people accused of crimes because it is one-sided.[195] While prosecutors and police have spent millions of dollars to build forensics labs, the New York Times reported that the majority of public defender offices do not have access to the equivalent forensic tools to test the prosecution's reports because they are underfunded, and because police "monopolize the experts in the field and forbid them from working for the defense."[196] The Legal Aid Society, based in New York, is the largest public defender agency in the U.S. and is the only office of its kind with a competitive digital forensics lab.[197] Other offices may have a single

---

iness/law-enforcement-public-defender-technology-gap.html [https://perma.cc/VMT4-3JQW]. The Manhattan District Attorney's office spent $10 million on their forensic lab in 2016. *Id.*

191. *See* Affidavit of John Logan Koepke at 4–5, Upturn v. New York City Police Dep't, No. 162380-2019 (N.Y. Sup. Ct. 2019); KOEPKE ET AL., *supra* note 148, at 41–42. A number of the crime-related extractions listed were reported to author by Jerome Greco, Supervising Attorney of the The Legal Aid Society's Digital Forensics Unit, and documented in redacted search warrants and court orders on file with the author.

192. *See, e.g.*, Ellen Yaroshefsky, *Cooperation with Federal Prosecutors: Experiences of Truth Telling and Embellishmen*t, 68 FORDHAM L. REV. 917, 945 (1999); *see also* KOEPKE ET AL., *supra* note 148, at 53.

193. *See infra* Section III.A.5.

194. *See* Hill, *supra* note 190.

195. *See id.*

196. *Id.*

197. *Id.*

extraction device or internal expert, but most defenders rely on outside consultants (in some jurisdictions, this requires judicial approval to authorize funding).[198]

Police and prosecutors are not the only state actors who subject black and brown people to disproportionate levels of surveillance that make their digital devices more likely to be monitored.[199] Social workers, teachers, doctors, lawyers, school "safety agents," security guards, and caseworkers are all more likely to surveil, search, and potentially digitally search Black individuals and other people of color.[200] Further:

> Black families are more likely to be reported to the child abuse hotline and investigated for child abuse and neglect. They are more likely to have cases against them substantiated and to have their children removed from their care. . . . Research shows these racial disparities, resulting in the overrepresentation of Black children in the child welfare system, are not due to a higher incidence of abuse and neglect in Black families as compared to white families.[201]

Doctors are more likely to drug test pregnant black women than white women, despite similar rates of substance use during pregnancy.[202] Schools with higher concentrations of students of

198. *Id.*

199. Laura T. Kessler, *"A Sordid Case":* Stump v. Sparkman*, Judicial Immunity, and the Other Side of Reproductive Rights*, 74 MD. L. REV. 833, 905–06 (2015).

200. *See* Dorothy Roberts & Lisa Sangoi, *Black Families Matter: How the Child Welfare System Punishes Poor Families of Color*, THE APPEAL (Mar. 26, 2018), https://theappeal.org/black-families-matter-how-the-child-welfare-system-punishes-poor-families-of-color-33ad20e2882 [https://perma.cc/9VYV-SVUZ]; *see also* Stephanie L. Rivaux et al., *The Intersection of Race, Poverty, and Risk: Understanding the Decision to Provide Services to Clients and to Remove Children*, 87 CHILD WELFARE 151, 165–66 (2008).

201. Roberts & Sangoi, *supra* note 200.

202. Ira J. Chasnoff et al., *The Prevalence of Illicit Drug or Alcohol Use During Pregnancy and Discrepancies in Mandatory Reporting in Pinellas County, Florida*, 322 NEW ENG. J. MED. 1202, 1205 (1990) ("Such variations in the reporting of women to public health authorities were evident in Pinellas County in the fact that a significantly higher proportion of black women than white women were reported, even though we found that the rates of substance use during pregnancy were similar."). "Providers' decisions to screen pregnant women for illicit substance use are influenced by both patients' characteristics and providers' personal attitudes. Hospital protocols might help reduce the potentially biased impact of attitudes on screening decisions." Bonnie D. Kerker et al., *Patients' Characteristics and Providers' Attitudes: Predictors of Screening Pregnant Women for Illicit Substance*

color are more likely to have "more intense security measures."[203] Receiving public entitlement benefits often exposes recipients to higher levels of state surveillance, such as purchase history tracking, home intrusions, and searches.[204] Some employers have begun requiring employees to wear Fitbits, for example, to monitor their physical activity.[205] While people may not want to use wearable devices like Fitbits, some employers have begun requiring their use with financial penalties for employees who do not comply.[206] For employees who cannot afford to lose their job, this surveillance technology is forced upon them.[207]

The wealth of information collected by digital devices and the power of police and other state agencies to conduct digital surveillance, combined with the dearth of resources in public defender offices to analyze such evidence, will result in a failure to protect many people from being convicted and incarcerated as a result of their pregnancy outcomes.[208] While we all share a certain level of privacy in our smartphones and personal computers, the legal status of that information, when shared with third-party internet providers and technology companies, remains uncertain.[209]

4. Legal status of evidence from digital devices

Unsurprisingly, given the rapid innovation in technology, the courts have lagged behind in creating protections around digital

---

Use, 28 CHILD ABUSE & NEGLECT 209, 210 (2004); *see also* Hillary Veda Kunins et al., *The Effect of Race on Provider Decisions to Test for Illicit Drug Use in the Peripartum Setting*, 16 J. WOMEN'S HEALTH 245 (Mar. 2007), at 5, https://www.ncbi.nlm.nih.gov/pmc/articles/PMC2859171/pdf/nihms-182195.pdf [https://perma.cc/HSN4-M55R].

203. Melinda D. Anderson, *When School Feels Like Prison*, THE ATLANTIC (Sept. 12, 2016), https://www.theatlantic.com/education/archive/2016/09/when-school-feels-like-prison/499556/ [https://perma.cc/Q5E7-F2YS].

204. *See* GELLMAN & ADLER-BELL, *supra* note 146, at 12.

205. Te-Ping Chen, *Your Company Wants to Know if You've Lost Weight*, WALL ST. J. (Feb. 11, 2019, 11:28 AM), https://www.wsj.com/articles/does-your-company-need-to-know-your-body-mass-index-11549902536 [https://perma.cc/P9QM-QAFT].

206. Ifeoma Ajunwa, *Algorithms at Work: Productivity Monitoring Applications and Wearable Technology as the New Data-Centric Research Agenda for Employment and Labor Law*, 63 ST. LOUIS UNIV. L.J. 21, 52 (2018).

207. *See id.*

208. *See supra* notes 195–98 and accompanying text.

209. MARY MADDEN & LEE RAINIE, PEW RES. CTR., AMERICANS' ATTITUDES ABOUT PRIVACY, SECURITY, AND SURVEILLANCE 3 (2015), https://www.pewresearch.org/internet/wp-content/uploads/sites/9/2015/05/Privacy-and-Security-Attitudes-5.19.15_FINAL.pdf [https://perma.cc/8ZG5-7WB3].

surveillance and forensics.[210] In *Riley v. California*, the U.S. Supreme Court acknowledged, for the first time, that modern cell phones "are now such a pervasive and insistent part of daily life that the proverbial visitor from Mars might conclude they were an important feature of human anatomy."[211] The *Riley* Court held that the police required a search warrant for the data stored on the phone in that case.[212] Four years later, the Court, in *Carpenter v. United States*, confronted the more complex question of whether police needed a search warrant to acquire data from cell phone towers that were pinged by the movement of an accused person's phone.[213] Police acquired the data by requesting information from the cell phone companies themselves, and this distinction allowed the government to argue that the accused waived any expectation of privacy because the cell phone companies were "third parties" with whom the accused shared information about their location.[214] The "third-party doctrine" tests for whether one retains a reasonable expectation of privacy in information shared with another party, and has generally prevented people seeking evidence suppression from claiming they retained privacy in documents shared with third parties.[215] Nevertheless, in *Carpenter,* argued by the American Civil Liberties Union (ACLU), the Court again found that the accused had a reasonable expectation of privacy in their data, despite having shared it with phone companies, and thus established precedent requiring additional constitutional protections.[216]

Specifically, the *Carpenter* Court recognized that our daily reliance on cellular devices and the "unique nature of cell phone location records" that wireless carriers record with detailed documentation, can paint a more detailed portrait than one any device-user is prepared to share.[217] The Court provided that:

> Mapping a cell phone's location over the course of 127 days provides an all-encompassing record of the holder's

210. *See* Mario Trujillo, *Computer Crimes*, 56 AM. CRIM. L. REV. 615, 649–51 (2019) (providing overview of federal statutes governing electronic monitoring); *see infra* notes 211–16 and accompanying text.
211. 573 U.S. 373, 385 (2014).
212. *See id.* at 403.
213. Carpenter v. United States, 138 S. Ct. 2206, 2221 (2018).
214. *See id.* at 2212, 2219.
215. *See* Smith v. Maryland, 442 U.S. 735, 743–44 (1979) (citing United States v. Miller, 425 U.S. 435, 443 (1976)).
216. *See Carpenter*, 138 S. Ct. at 2217–19.
217. *Id.*

> whereabouts. As with GPS information, the time-stamped data provides an intimate window into a person's life, revealing not only his particular movements, but through them his "familial, political, professional, religious, and sexual associations."[218]

This distance between the intimate level of information we all entrust in our phones and the lack of legal protections for that information currently makes us all vulnerable to our data being used against us in unforeseen ways.[219]

i. Post-Carpenter *applications to other digital data.*

Courts' application of *Carpenter* to other digital data, like search engine queries, purchasing history, and health data from wearable devices, is still developing.[220] Post-*Carpenter*, federal courts in the First and Fifth Circuits,[221] Arizona,[222] Rhode Island,[223] Minnesota[224], Washington,[225] New York,[226] Louisiana,[227] and Georgia[228] have

---

218. *Id.* at 2217. For some of the things police could determine about someone from just their location information, including accessing an abortion clinic, *see* People v. Weaver, 909 N.E.2d 1195, 1999 (N.Y. 2009).

> Disclosed in [GPS] data . . . will be trips the indisputably private nature of which takes little imagination to conjure: trips to the psychiatrist, the plastic surgeon, the abortion clinic, the AIDS treatment center, the strip club, the criminal defense attorney, the by-the-hour motel, the union meeting, the mosque, synagogue or church, the gay bar and on and on.

Id.

219. *See Weaver*, 909 N.E.2d at 1200.
220. *See infra* text accompanying notes 221–55.
221. *See* United States v. Hood, 920 F.3d 87, 91–92 (1st Cir. 2019); *see also* United States v. Contreras, 905 F.3d 853, 857 (5th Cir. 2018).
222. United States v. McCutchin, No. CR-17-01417-001-TUC-JAS (BPV), 2019 WL 1075544, at *2–3 (D. Ariz. Mar. 7, 2019). *But see* State v. Mixton, 447 P.3d 829, 836–37, 841 (Ariz. Ct. App. 2019) (finding no federal expectation of privacy but holding the state constitution protected IP address subscriber information).
223. United States v. Monroe, 350 F. Supp. 3d 43, 48–49 (D.R.I. 2018) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018)).
224. United States v. James, No. 18-CR-216 (SRN/HB), 2018 WL 6566000, at *4 (D. Minn.), *aff'd*, No. 18-CR-216 (SRN/HB), 2018 WL 6529492 (D. Minn. Dec. 11, 2018), *vacated*, (Dec. 13, 2018), *aff'd*, No. 18-CR-216 (SRN/HB), 2019 WL 325231 (D. Minn. Jan. 25, 2019).
225. United States v. Barnes, No. CR18-5141, 2019 WL 2515317, at *5 (W.D. Wash. June 18, 2019).

continued to treat requests by police to Internet Service Providers (or "ISPs") regarding users' Internet Protocol address (or "IP address") differently than requests to cell phone companies for cell phone tower location data. Courts have based the treatment on various distinctions, most emphatically that ISP requests for IP address subscriber information are not as comprehensive as cell phone company requests for location data and that IP addresses, without more, do not reveal the user's exact location history.[229]

Courts have also declined to extend the protections outlined in *Carpenter* based on how voluntary an accused's engagement was with a platform from which police are obtaining information.[230] For example, while a Minnesota court held that an accused user of a peer-to-peer network (i.e., Napster, LimeWire, etc.) had an expectation of privacy in his anonymous account, it also held that even under *Carpenter's* higher level of scrutiny, he abandoned any right to privacy by using peer-to-peer software, even if he didn't share the files directly with the program.[231] A Pennsylvania court, despite a

226. United States v. Kidd, 394 F. Supp. 3d 357, 362–64 (S.D.N.Y. 2019); Brown v. Sprint Corp. Sec. Specialist, 17-CV-2561(JS)(ARL), 2019 WL 418100, at *4 (E.D.N.Y Jan. 31, 2019).

227. United States v. Felton, 367 F. Supp. 3d 569, 574–75 (W.D. La. 2019).

228. United States v. Jenkins, No. 18-CR-181-MLB-CMS, 2019 WL 2482171, at *2 (N.D. Ga.), *aff'd*, No. 18-CR-00181, 2019 WL 1568154 (N.D. Ga. Apr. 11, 2019).

229. *See* United States v. Monroe, 350 F. Supp. 3d 43, 48 (D.R.I. 2018) (quoting Carpenter v. United States, 138 S. Ct. 2206, 2219 (2018)) ("The FSS's record of Monroe's IP address was not an 'exhaustive chronicle' of his physical or digital activities."); *see also Kidd*, 394 F. Supp. 3d at 362 ("Although here the Government sought IP address information for a substantial amount of time and for an inherently mobile device, Kidd has failed to demonstrate that fact translated into surveillance of Kidd's daily movements . . . ."); *see also* United States v. Hood, 920 F.3d 87, 91 (1st Cir. 2019) ("Hood does not dispute that he voluntarily disclosed the information to Kik that he now seeks to suppress."). *But see* State v. Mixton, 447 P.3d 829, 842 (Ariz. Ct. App. 2019) (under Arizona state constitution protection of "private affairs," "internet users generally have an expectation of privacy in their subscriber information. . . . Warrantless government collection of this information from an internet service provider or similar source thus constitutes a significant and unwarranted intrusion into a person's private affairs—an intrusion our constitution unambiguously prohibits."); *see also* State v. Reid, 945 A.2d 26, 33–34 (N.J. 2008) (affirming suppression under state constitutional for warrantless request to ISP for IP address subscriber information).

230. *See infra* text accompanying notes 231–32.

231. United States v. Shipton, No. 18-CR-202-PJS, 2019 WL 5330928, at *14 (D. Minn.) (holding that child rescue coalition surveillance tools did not violate *Carpenter*, with detailed history and operational overview of Child Rescue Coalition software), *aff'd*, No. 18-CR-0202 (PJS/KMM), 2019 WL 5305573 (D. Minn. Oct. 21, 2019).

concurring justice recognizing that "[a]n Internet search and browsing history, for example, can be found on an Internet-enabled [personal computer] and could reveal an individual's private interests or concerns—perhaps a search for certain symptoms of disease, coupled with frequent visits to WebMD," nevertheless held that child pornography found by a repair shop was the type of voluntary sharing of digital evidence that abandoned any right to privacy.[232]

At least one court post-*Carpenter* recognizes that a great deal of legitimately private information is stored in both smartphones and on search engine servers, signaling perhaps a more nuanced approach to IP addresses.[233] Declining to apply *Carpenter's* protections to a case challenging the retrieval of subscriber information from an IP address, one District Court judge at least "caution[ed] against the categorical approach found in most of the post-*Carpenter* cases holding that there is no reasonable expectation of privacy in IP address information."[234] Yet the judge still held that the accused failed to meet the *Carpenter* burden, as he and many other judges interpret it to mean that the information sought from an IP address alone must reveal physical movements.[235] This standard fails to appreciate the relevance of digital evidence to the similarly revealing online movements from search page, to website, to linked resource, to video, to comments below videos linked to another page, etc.—which is often more valuable and more revealing information for the government than an accused's physical location history.[236] "[E]ven if IP addresses cannot physically 'track' people about town, they can still show one's digital travels, personal curiosities, and online associations."[237] One does not need to physically visit the abortion clinic, the Alcoholics Anonymous meeting, a doctor, the library, the union hall, or a political office in order for a government agent to glean one's "familial, political, professional, religious, and sexual associations" from his or her search engine history.[238] What one has

232. Commonwealth v. Shaffer, 209 A.3d 957, 989 (Pa. 2019) (Wecht, J., concurring in part) (quoting Riley v. California, 573 U.S. 373, 395–96 (2014)); *see also id.* at 977 (detailing the holding).

233. *See* United States v. Kidd, 394 F. Supp. 3d 357, 368 (S.D.N.Y. 2019).

234. *Id.*

235. *Id.* at 367–68.

236. Michael Price and William Wolf, *Building on* Carpenter*: Six New Fourth Amendment Challenges Every Defense Lawyer Should Consider*, NAT'L ASS'N OF CRIM. DEF. LAWS. (July 28, 2019), https://www.nacdl.org/Content/Building-on-Carpenter-Six-New-Fourth-Amendment-Cha [https://perma.cc/PG6A-LWZC].

237. *Id.*

238. Carpenter v. United States, 138 S. Ct. 2206, 2217 (2018) (quoting United States v. Jones, 565 U.S. 400, 415 (2012) (Sotomayor, J., concurring)).

researched—whether medication based abortions, abortion procedures, anatomy, people, or places—reveals one's internal dialogue and intent arguably more closely than what one may infer from another's physical location history.[239] Fortunately, assuming no exceptions apply, some state constitutions have filled the gap and given state court judges a basis for suppressing subscriber information from IP addresses without a warrant.[240]

Similarly, search or web browsing history obtained either through the device or from the search engine should also be protected under *Carpenter* because "the deeply revealing nature of [the data]" and "its depth, breadth, and comprehensive reach . . . does not make it any less deserving of Fourth Amendment protection."[241] "Tracking cookies, like historical [cell site location information], have outgrown the confines delineated by *Miller* and *Smith* that have failed to accommodate new, 'distinct categor[ies] of information' born from 'the seismic shifts in digital technology.'"[242]

Besides subscriber information through IP addresses, police have also tried to obtain an accused's purchasing history as evidence of a crime.[243] An Oregon court declined to extend *Carpenter* to an accused's purchasing history on the online platform eBay, again narrowing *Carpenter's* protections to location data controlled by third parties.[244] The court held that "[w]hen [the accused] used the online platform, he voluntarily conveyed his purchasing information

239. *See id.* at 2223.

240. State v. Mixton, 447 P.3d 829, 837, 842 (Ariz. Ct. App. 2019) (Under Arizona state constitution protection of "private affairs," "[w]arrantless government collection of this information from an internet service provider or similar source thus constitutes a significant and unwarranted intrusion into a person's private affairs—an intrusion our constitution unambiguously prohibits."); State v. Reid, 945 A.2d 26, 34, 38 (N.J. 2008) ("internet users have a reasonable expectation of privacy in their subscriber information . . .") (affirming suppression under state constitution of warrantless request to ISP for IP address subscriber information).

241. *Carpenter*, 138 S. Ct. at 2223.

242. Daniel de Zayas, Comment, Carpenter v. United States *and the Emerging Expectation of Privacy in Data Comprehensiveness Applied to Browsing History*, 68 AM. U. L. REV. 2209, 2249 (2019) (quoting *Carpenter* 138 S. Ct. at 2219).

243. *See infra* notes 244–45 and accompanying text; *see also supra* notes 9–11, 16, 127–29, 178–79 and accompanying text; *see infra* discussion at III.A.6 (particularly note 314 and accompanying text).

244. United States v. Schaefer, No. 17-cr-00400, 2019 WL 267711, at *5 (D. Or. Jan. 17, 2019).

to the company and 'exposed' that information to the company in the ordinary course of business."[245]

However, an Illinois court held that a warrant is required for law enforcement to obtain smart-meter electricity data obtained by the city.[246] In *Naperville*, the Seventh Circuit held that the smart-meter was comparable to the thermal imaging in *Kyllo v. United States*[247] and that reading them could reveal "when people are home, when people are away, when people sleep and eat, what types of appliances are in the home, and when those appliances are used."[248] Due to the invasiveness of the smart-meter reading and lack of choice in submitting information to it, the third-party doctrine did not block suppression.[249] Advocates in future technology cases should similarly pull from other pre-*Carpenter* cases for principles that promote stronger privacy protections from state surveillance not limited to revealing location data.[250]

Another avenue advocates should explore to strengthen legally recognized expectations of privacy include technologies that hold medical information, like menstrual cycle apps, wearable devices that track heart rate and physical activity, and internet searches for medical information.[251] Whether *Carpenter* will protect information related to a pregnant person's web searches for information about their reproductive health depends on how the courts treat medical information sought online under the third-party doctrine.[252] Medical records are of course covered by the Health Insurance Portability and Accountability Act (HIPAA),[253] and courts have held that patients retain privacy interests in their records despite the medical facility having custody of those records.[254] The ACLU made a strong

245. *Id.*; *see also* United States v. Therrien, No. 18-cr-00085, 2019 WL 1147479, at *3 (D. Vt. Mar. 13, 2019) (declining to extend *Carpenter* to Google search history).

246. Naperville Smart Meter Awareness v. City of Naperville, 900 F.3d 521, 528–29 (7th Cir. 2018).

247. *Id.* at 525–26 (citing Kyllo v. United States, 533 U.S. 27, 40 (2001)).

248. *Id.* at 526.

249. *Id.* at 527.

250. *See* cases cited *infra* note 254.

251. Carrie N. Baker, Opinion, *Period Tracking Apps in an Age of Anti-Abortion Government Surveillance*, DAILY HAMPSHIRE GAZETTE, (Jan. 22, 2020, 6:00 PM), https://www.gazettenet.com/Columnist-Carrie-N-Baker-Period-Tracking-Apps-in-an-Age-of-Anti-Abortion-Government-Surveillance-32172538 [https://perma.cc/3JV9-NTK9].

252. *See infra* text and accompanying notes 256–60.

253. Health Insurance Portability and Accountability Act of 1996 (HIPAA), Pub. L. No. 104–191, § 1173(d)(2), 110 Stat. 1936, 2026.

254. *See* Tucson Woman's Clinic v. Eden, 379 F.3d 531, 550–51 (9th Cir. 2004) (requiring warrant for search of medical records in abortion clinic because "all provision of

argument in an amicus brief that the Drug Enforcement Administration (DEA) unlawfully sought patient records from a prescription drug database for a criminal investigation via an administrative subpoena.[255]

It is clear that patients retain privacy interests in their medical records despite third-party custody, but medical providers are no longer the only repositories of medical information.[256] As discussed above, even though the majority of Americans who use their smartphones, computers, "Internet of Things" devices (i.e., Alexa, Smart Home devices, etc.), and wearable devices for medical advice and health tracking, might reasonably believe that this information would be considered very, or at least "somewhat sensitive," it does not change the fact that we are sharing our sensitive medical data with third parties.[257] Privacy advocates will need to argue that the nature of the information contained in devices sought by law enforcement is private, sensitive, and confidential, that society generally recognizes it as private, as well as arguing that the person whose data is sought involuntarily allowed a third-party to hold it in its custody.[258] As the ACLU argued in *Jonas*, "[t]he decision to visit a physician and pharmacist to obtain urgent medical treatment is not in any meaningful sense voluntary."[259] If a person is seeking online reproductive health advice because they have few local alternatives, then perhaps one could argue that virtual medicine was one's only alternative and that "there is no way to avoid leaving behind a trail of [medical] data."[260]

---

medical services in private physicians' offices carries with it a high expectation of privacy for both physician and patient"); *see also* Ferguson v. City of Charleston, 532 U.S. 67, 78, 86 (2001) (holding urine tests were "searches" within meaning of Fourth Amendment and reporting of test results indicating cocaine use to police were unreasonable searches).

255. *See* Brief for American Civil Liberties Union et al. as Amici Curiae in Support of Respondent-Appellant at 3, U.S. Dep't of Just. v. Ricco Jonas, No. 19-1243 (1st Cir. May 29, 2019) [hereinafter Brief in Support of Respondent-Appellant].

256. *See supra* note 215 and accompanying text.

257. MARY MADDEN, PEW RSCH. CTR., PUBLIC PERCEPTIONS OF PRIVACY AND SECURITY IN THE POST-SNOWDEN ERA 31–39 (2014), https://www.pewresearch.org/wp-content/uploads/sites/9/2014/11/PI_PublicPerceptionsofPrivacy_111214.pdf [https://perma.cc/DY4V-BZ5J].

258. *See* United States v. Miller, 425 U.S. 435 (1976); *see also* Smith v. Maryland, 442 U.S. 735 (1979).

259. Brief in Support of Respondent-Appellant, *supra* note 255, at 11.

260. *Id.* at 12 (quoting Carpenter v. United States, 138 S. Ct. 2206, 2220 (2018)).

ii. Scope of search warrants for digital data.

In cases where the government serves a judicial search warrant, advocates should narrow the scope of the search warrant.[261] In what one scholar coined the "Magistrate's Revolt," judges "began to include constraints on how the government could execute digital searches in the warrants that they issued."[262] The constraints include requiring justifications for seizures of specific hardware (rather than allowing seizures of all devices), constraints on the timeframe that police can search devices,[263] constraints on the timeframe of the search query,[264] the data relevant to the search,[265] the search methods (e.g., keywords, file types),[266] etc.[267]

For defenders of pregnant people whose devices have been seized pursuant to a search warrant, they should fight to narrow the devices that can be searched, narrow the amount of time detectives have to perform their search, add language to the search warrant narrowing the query by time frame, by file type and data sought, by what crime is suspected to be established through the search of the device, and as many other specificities as possible.[268]

---

261. *See* United States v. Dichiarinte, 445 F.2d 126, 129–30 (7th Cir. 1971).

262. Emily Berman, *Digital Searches, the Fourth Amendment, and the Magistrates' Revolt*, 68 EMORY L.J. 49, 61 (2018).

263. United States v. Ganias, 755 F.3d 125, 137–38 (2d Cir. 2014), *reh'g granted en banc*, 824 F.3d 199 (2d Cir. 2016) ("without some independent basis for its retention of those documents in the interim, the Government clearly violated Ganias's Fourth Amendment rights by retaining the files for a prolonged period of time and then using them in a future criminal investigation.").

264. People v. Thompson, 178 A.D.3d 457, 458 (N.Y. App. Div. 2019) (holding search warrant for phone overly broad when it failed to specify time limitation).

265. Carter v. State, 105 N.E.3d 1121, 1130 (Ind. Ct. App. 2018) ("[T]he warrant specifically described the place law enforcement could search—the phone recovered from Carter—and specifically described what law enforcement could search for—(1) 'any information relating to calls, messages, including Facebook messages and accounts,' and (2) 'all information . . . that would indicate the identity of the phone's owner/user.").

266. United States v. Carey, 172 F.3d 1268, 1272–73 (10th Cir. 1999) ("The warrant obtained for the specific purpose of searching defendant's computers permitted only the search of the computer files for 'names, telephone numbers, ledgers, receipts, addresses, and other documentary evidence pertaining to the sale and distribution of controlled substances.' The scope of the search was thus circumscribed to evidence pertaining to drug trafficking.").

267. *See* Berman, *supra* note 262, at 61–62.

268. *See* United States v. Dichiarinte, 445 F.2d 126, 129–30 (7th Cir. 1971). Further complicating the role that digital evidence plays in the courts is that the source of some digital evidence comes from third-party privately developed software. *See* Carpenter v. United States, 138 S. Ct. 2206, 2214 (2018). When defense attorneys subpoena the software to analyze why the evidence its producing implicates the

iii. Scope of consent to searches of digital data.

As discussed above, pregnant people should be counseled not to voluntarily share their digital devices with hospitals or law enforcement.[269] If they already have shared a device, as many people commonly do, advocates can still argue that the search conducted lacked knowing and voluntary consent, or was broader than what the person handing over their device believed they consented to.[270] For example, in cases about searches of automobiles, where the "consent" was limited in scope to what may be in the trunk, the back seat, or the center console, courts have held that the scope of consent did not extend to all parts of the car.[271] Similarly, advocates should argue that to the extent a digital device was voluntarily relinquished to the police, the reasonable expectation of the accused was not for every piece of data on the phone to be analyzed and digested into a two-thousand page digital trail of everything they have done in real life and online.[272] This requires a detailed factual analysis of the circumstances, the area being consented to a search within, the exact words said which illustrate that understanding, the reasonable meaning of those words in that context, and other details.[273]

The legal status of pregnant people's reasonable expectation of privacy—while still somewhat undetermined—will challenge advocates to protect their information absent additional state constitutional provisions and state laws protecting the privacy of online information along the same lines as protection for self-incriminating statements under the Fifth Amendment of the U.S. Constitution.[274] The types of remedies needed include: suppression motions, which will prevent prosecutions based on unlawfully

---

accused, they are often met by a motion to quash the subpoena from the company's law firm. *See* Rebecca Wexler, *Life, Liberty, and Trade Secrets: Intellectual Property in the Criminal Justice System*, 70 STAN. L. REV. 1343, 1349–50 (2018).

269. *See supra* note 268 and accompanying text.

270. *See* H. Patrick Furman, *The Consent Exception to the Warrant Requirement*, 23 COLO. LAW., 2105, 2106 (1994); *see also* KOEPKE ET AL., *supra* note 148, at 46–47 (discussing percentage of extractions based on consent in various cities across the U.S. between 2015 and 2019).

271. *See, e.g.*, Florida v. Jimeno, 500 U.S. 248, 251 (1991).

272. *See* United States v. Heckenkamp, 482 F.3d 1142, 1146 (9th Cir. 2007).

273. *See* United States v. Ross, 456 U.S. 798, 808–09 (1982).

274. *See* Janelle T. Wilke, Comment, *The Fourth Amendment, a Woman's Right: An Inquiry into Whether State-Implemented Transvaginal Ultrasounds Violate the Fourth Amendment's Reasonable Search Provision*, 18 CHAP. L. REV. 921, 934 (2015); *see also, e.g.*, Coulon, *supra* note 167, at 86–87 (providing an example where an individual may invoke right against self-incrimination).

obtained information;[275] private rights of action that will compensate people whose rights have been violated;[276] the ability to sue anonymously to avoid deterring plaintiffs claiming privacy violations;[277] and standing for stakeholder organizations to bring claims on behalf of groups of people whose rights were violated.[278]

5. Digital data has already been used against women as evidence of self-induced abortions.

Laws prohibiting self-induced abortion already make women vulnerable to surveillance and prosecution for taking abortion pills in some states, and as discussed above in Part II,[279] the probability of new laws criminalizing abortion-related conduct is high.[280] Pregnant people seeking to terminate a pregnancy are trackable in multiple ways through their digital devices.[281] Search browsing history, unencrypted communications, location history, purchasing history, databases for state police, welfare, and child protective services, social media activity, smart home devices, wearable devices, and menstrual tracking apps all store information relevant to pregnant people's reproductive health and decisions.[282]

Evidence of one woman's search engine history from her phone has already been introduced to support the state of Mississippi's indictment of her.[283] In April 2017, Latice Fisher's husband called 911 to report that his wife had possibly delivered a baby at home.[284] When EMTs arrived, they found a 35-week-old and six-pound fetus with "no signs of life, . . . blue skin and no heartbeat."[285] Ms. Fisher then went with the EMTs to the hospital.[286] She was later indicted on

275. *See* United States v. Lisbon, 835 F. Supp. 2d 1329, 1360–61 (N.D. Ga. 2011).
276. *See* Judith A. McMorrow, *Who Owns Rights: Waiving and Settling Private Rights of Action*, 34 VILL. L. REV. 429, 434–35 (1989).
277. *See* NAT'L CRIME VICTIM L. INST., PROTECTING VICTIMS' PRIVACY RIGHTS: THE USE OF PSEUDONYMS IN CIVIL LAW SUITS 1–2 (2011), https://law.lclark.edu/live/files/11778-protecting-victims-privacy-rights-the-use-of [https://perma.cc/738C-VZEV].
278. *See generally*, Rosa Kusbiantoro, *Human Rights, Access to Remedy, and Stakeholder Engagement*, BSR: BLOG (June 18, 2019), https://www.bsr.org/en/our-insights/blog-view/human-rights-access-to-remedy-and-stakeholder-engagement [https://perma.cc/4XUL-DH83].
279. *See supra* Section II.A.
280. *See* The SIA Legal Team, *supra* note 48, at 5.
281. *See id.* at 23.
282. *Id.*
283. *See* Phillips, *supra* note 3.
284. *Id*.
285. *Id*.
286. *Id.*

a second-degree murder charge in January 2018 under the theory that the fetus died due to asphyxiation after being born alive, and detained under $100,000 bail, facing twenty to forty years of incarceration and possibly life in prison.[287] She was later released on bond in March of 2018.[288] The state's theory that there had been a live birth was based on a "lung float test" which had been used to determine whether the lungs respirated.[289] After the National Advocates for Pregnant Women and local counsel brought to the state's attorney attention that this test lacks scientific validity—with support from vigorous organizing efforts by Color of Change and the Mississippi Freedom Fund—he dismissed the murder charges in May 2019 without prejudice.[290] A Grand Jury rejected the District Attorney's second attempt at indicting Ms. Fisher for manslaughter in March 2020.[291]

The state's evidence in its first presentation included that in her third trimester, Ms. Fisher "conduct[ed] internet searches, including how to induce a miscarriage, 'buy abortion pills, mifepristone online, misoprostol online,' and 'buy misoprostol abortion pill online,'" and purchased misoprostol online.[292] Without the information in her phone, it seemed clear that the State would have insufficient evidence to sustain a prosecution.[293] Her digital data gave prosecutors a "window into [her] soul"[294] to substantiate their general theory that she did not want the fetus to survive even if the abortion medication she pursued would have been unable to terminate her pregnancy in the third trimester.[295]

Another woman, Purvi Patel, was sentenced to twenty years in prison for "neglect of a dependent and feticide" after taking abortion pills she purchased online.[296] Evidence presented against her at trial

287. *Id.*; Teddy Wilson, *Mississippi Woman Criminally Charged for Pregnancy Outcome After Home Birth (Updated)*, REWIRE NEWS GRP., https://rewire.news/article/2018/02/06/mississippi-woman-criminally-charged-pregnancy-outcome-home-birth/ [https://perma.cc/7L3Z-UK2N] (last updated Apr. 13, 2018, 12:56 PM).
288. *See* Phillips, *supra* note 3.
289. *Id.*
290. *Id.*
291. *See* A No Bill, *supra* note 11.
292. *See* Phillips, *supra* note 3.
293. *Id.*
294. *See* Adams, *supra* note 184.
295. *See* Phillips, *supra* note 3.
296. Becca Costello, *Indiana Court Overturns Feticide Conviction of Purvi Patel*, THE WORLD (July 22, 2016 2:00 PM), https://www.pri.org/stories/2016-07-22/indiana-court-overturns-feticide-conviction-purvi-patel [https://perma.cc/HAN7-HAWT].

included online research she conducted, the email confirmation she received from internationaldrugmart.com, and unencrypted text messages to a friend about her relationship, becoming pregnant, and the pills she purchased.[297] While Patel's conviction for feticide was overturned (the Court ruled the legislature did not intend for a pregnant woman to be charged for her own feticide), she was still convicted of "neglect of a dependent" and spent more than three years detained.[298] Once again, without her digital evidence, the prosecutor would only have been able to pursue her conviction based on medical testimony from her treatment providers and experts.[299] Instead, the prosecutor introduced Ms. Patel's smartphone and iPad—which both contained text messages and emails—as evidence against her.[300]

Digital evidence fills a gap for prosecutors keen on prosecuting women for their pregnancy outcomes.[301] When medical theories fail

297. *See* Patel v. State, 60 N.E.3d 1041, 1047 (Ind. Ct. App. 2016); *see* Aziza Ahmed, *Floating Lungs: Forensic Science in Self-Induced Abortion Prosecutions*, 100 B.U. L. REV. 1111, 1127 (2020).

298. Cleve R. Wootson Jr., *Court Overturns Feticide Conviction of Indiana Woman Who Had Self-Induced Abortion*, WASH. POST (July 22, 2019, 3:02 PM), https://www.washingtonpost.com/news/post-nation/wp/2016/07/22/court-overturns-feticide-conviction-of-indiana-woman-who-had-self-induced-abortion/ [https://perma.cc/9M74-8UQV].

299. *See supra* note 297 and accompanying text; *see also infra* notes 301–02 and accompanying text.

300. Kelli Stopczynski, *Prosecutors: Text Messages Detail Weeks Leading Up to Patel's Forced Abortion*, WSBT (Apr. 2, 2015), https://wsbt.com/news/local/prosecutors-text-messages-detail-weeks-leading-up-to-patels-forced-abortion [https://perma.cc/3DYV-XM8H].

301. *See* Rankin, *supra* note 11. Two other women prosecuted for their pregnancy outcomes based partially on digital evidence include Roberta Baker and Brook Skyler Richardson. *See* Matt McFarland, *Mother Goes to Trial for Infant's Death* , DAILY J., https://dailyjournalonline.com/news/local/crime-and-courts/mother-goes-to-trial-for-infants-death/article_20a8de66-ef1f-5a02-88c4-73b9c52560e4.html [https://perma.cc/Y8PM-WCEJ] (June 27, 2019) (detailing use of Baker's messages and Facebook photo of baby to argue personal knowledge of medical vulnerability); *see* Kieth BieryGolick & Cameron Knight, *Ex-Cheerleader Accused of Killing Newborn Found Not Guilty on Most Serious Charges*, USA TODAY, https://www.usatoday.com/story/news/nation/2019/09/12/brooke-skylar-richardson-trial-not-guilty-most-serious-charges/2305221001/ [https://perma.cc/E4SV-Z7Z7] (Sept. 12, 2019, 5:56 PM). Ms. Richardson's text messages with her mother about her weight were introduced to demonstrate her vanity about her body during pregnancy, plus "searches on Richardson's phone for 'what happens at the gyno when your (sic) pregnant.'" Abby Dawn, *Brooke Skylar Richardson to Authorities in 2017 Interview: 'I think I killed her … I squeezed her'*, WCPO CINCINNATI, https://www.wcpo.com/news/local-news/warren-county/lebanon/week-2-of-brooke-skylar-richardsons-murder-trial-begins [https://perma.cc/J7ZJ-HQB9] (Sept. 9, 2019, 9:30PM).

to explain why some outcomes happened, prosecutors can now sift through an accused person's most personal thoughts, feelings, movements, and medically-related purchases during their pregnancy, even if there is little evidence supporting the conclusion that their conduct caused the pregnancy to end.[302]

Miscarriages naturally terminate up to 21% of pregnancies after week five and as many as 75% of pregnancies before week five; thus, it is not uncommon for a woman contemplating an abortion to coincidentally suffer a miscarriage.[303] Corporate and state access to our digital diaries is a dangerously unregulated area of law, with the potential to allow the pregnant people to be caught under a large net of surveillance regarding our most intimate thoughts.[304]

6. Other types of digital data that could potentially be used to criminalize pregnant people.

Additional types of data may also be used against pregnant people and their abortion providers in the future.[305] As already discussed, location history is available both through digital device extractions and subpoenas to cell phone tower companies.[306] Pregnant people's locations can also be identified by geofencing, an advertising tool used to market products based on the consumer's location.[307] Geofencing tools have already targeted people entering and leaving Planned Parenthood clinics across the country, sending them anti-abortion messages via their search browser on their digital devices.[308]

---

302. *See* Rankin, *supra* note 11.

303. Zawn Villines, *What Are the Miscarriage Rates by Week?*, MED. NEWS TODAY (Jan. 12, 2020), https://www.medicalnewstoday.com/articles/322634#pregnancy-loss-rates-by-week [https://perma.cc/5R2V-KLHW].

304. *See, e.g.*, *infra* note 309 and accompanying text.

305. *See* Aaron Pressman, *Anti-Abortion Group Sends Targeted Ads to Women in Planned Parenthood Clinics*, FORTUNE (May 26, 2016, 12:10 PM), https://fortune.com/2016/05/26/anti-abortion-groups-planned-parenthood/ [https://perma.cc/Q7RA-WB46]. Indeed, it's possible it has been, and the authors are unaware. *Id.*

306. *See* Carpenter v. United States, 138 S. Ct. 2206, 2212 (2018) (explaining cell site location information).

307. *See* White, *supra* note 20.

308. *See* Sharona Coutts, *Anti-Choice Groups Use Smartphone Surveillance to Target 'Abortion-Minded Women' During Clinic Visits*, REWIRE NEWS GRP. (May 25, 2016, 6:52 PM), https://rewire.news/article/2016/05/25/anti-choice-groups-deploy-smartphone-surveillance-target-abortion-minded-women-clinic-visits/ [https://perma.cc/4D8J-JT86]; *see* Christina Cauterucci, *Anti-Abortion Groups Are Sending Targeted Smartphone Ads to Women in Abortion Clinics*, SLATE (May 26, 2016, 4:31 PM), https://slate.com/human-interest/2016/05/anti-abortion-groups-are-sending-targeted-smartphone-ads-to-women-in-abortion-clinics.html [https://perma.cc/8BMF-M8WV].

In the criminal context, prosecutors have attempted to use reverse geofencing technology to identify a suspect of a bank robbery by serving Google with a search warrant to produce information on every person whose location services indicated they were within a radius of the bank around the time of the robbery.[309]

Digital advertising broker companies in general are also amassing and redistributing large amounts of highly sensitive medically related data.[310] For example, "a company named MedBase 200 reportedly used 'proprietary models' to generate and sell marketing lists of rape victims, domestic abuse victims, and patients with hundreds of different illnesses."[311] Other advertising services sell products that allow a company to buy information about all the clicks users make on every website, also inferring demographics about each user (e.g., gender and age based on browsing behavior).[312] While this type of service is supposed to protect users' personally identifiable information, there are "[n]umerous articles and academic studies [showing] how it is possible to unmask people using so-called anonymized data."[313]

As mentioned above, pregnant people's purchasing history—whether produced through credit cards or public benefits cards—is also susceptible to profiling them as pregnant, allowing surveillance of what food they buy and locations where they make purchases.[314]

---

309. Frank Green, *Defense Challenges Use of Google Location Data from Everyone in Vicinity of Hull Street Road Bank Robbery*, RICH. TIMES-DISPATCH (Jan. 22, 2020), https://richmond.com/news/local/crime/defense-challenges-use-of-google-location-data-from-everyone-in/article_9e4f9ca6-d092-5f07-b932-b111553a114d.html [https://perma.cc/4YRK-UD8K]. In Chatrie's case, the warrant sought location histories kept by Google of cellphones and other devices used within 150 meters (roughly 500 feet) of the bank during a period of one to two hours surrounding the time of the crime. *See id.*

310. *See* Neal Ungerleider, *The Latest Privacy Risk? Looking Up Medical and Drug Information Online*, FASTCO. (Feb. 23, 2015), https://www.fastcompany.com/3042763/privacy-risk-looking-up-medical-health-information-online [https://perma.cc/6U7K-YAVH].

311. *Id.*

312. *See* Joseph Cox, *Leaked Documents Expose the Secret Market for Your Web Browsing Data*, VICE (Jan. 27, 2020, 9:00 AM), https://www.vice.com/en_us/article/qjdkq7/avast-antivirus-sells-user-browsing-data-investigation?utm_source=First+Draft+Subscribers&utm_campaign=44ad290336-EMAIL_CAMPAIGN_2019_10_29_11_33_COPY_01&utm_medium=email&utm_term=0_2f24949eb0-44ad290336-265444013&mc_cid=44ad290336&mc_eid=949a99f398 [https://perma.cc/KG3A-MTD8].

313. *Id.*

314. *See* Wootson, *supra* note 298. "In 2014, Maine Gov. Paul LePage released data to the public detailing over 3,000 transactions from welfare recipients using EBT cards in

Beyond purchasing history collected by state agencies, a vast amount of personal, private, and medical information is also collected by the state.[315] These databases are increasingly broad and interconnected.[316] "Complex integrated databases collect [poor and working class people's] most personal information, with few safeguards," and "[v]ast complexes of social service, law enforcement, and neighborhood surveillance [that] make their every move visible and offer up their behavior for government, commercial, and public scrutiny."[317] The Alleghany Family Screening Tool, for example, was built by integrating multiple databases from state and county programs.[318]

> Twenty-nine different programs—including adult probation, the bureau of drug and alcohol services, the housing authority, the county jail, the juvenile probation office, the Allegheny County police department, the state office of income maintenance, the office of mental health and substance abuse services, the office of unemployment compensation, and almost 20 local school districts—send regular data extracts. The extracts include client names, social security numbers, dates of birth, addresses, and the type and amount of services they've received.[319]

Social media activity—including posts, but also likes, shares, comments on other posts, etc.—can also be extracted by investigators for evidence of what a pregnant person was thinking of or feeling around the time of the pregnancy outcome for which they may be

---

the state." Virginia Eubanks, *How Big Data Is Helping States Kick Poor People Off Welfare*, NEW AM. (Feb. 6, 2018), https://www.newamerica.org/fellows/in-the-news/how-big-data-helping-states-kick-poor-people-welfare/ [https://perma.cc/ZJ8B-7JTK]. Governor LePage used the data collection ability of the EBT cards to compile data on each time EBT's were used in a strip club, liquor store, smoke shop, or bar, arguing for a decrease in state welfare spending. *See id.*

315. *See* Dennis Anon, *What Does the US Government Know About You?*, PRIVACY.NET (Feb. 17, 2018), https://privacy.net/us-government-surveillance-spying-data-collection/ [https://perma.cc/MT2U-EY27].

316. *See id.*

317. VIRGINIA EUBANKS, AUTOMATING INEQUALITY: HOW HIGH-TECH TOOLS PROFILE, POLICE, AND PUNISH THE POOR 11 (2018).

318. *A Response to Allegheny County DHS*, VIRGINIA EUBANKS (Feb. 16, 2018), https://virginia-eubanks.com/2018/02/16/a-response-to-allegheny-county-dhs/ [https://perma.cc/96T3-6BZ4].

319. EUBANKS, *supra* note 317, at 135.

under investigation.[320] To search social media platforms, many police departments do not need access to a device; social media platforms grant them special access to perform keyword searches on posts geotagged within their jurisdiction.[321] Some social scientists have even attempted to perform predictive analytics on the language used in social media posts to predict future violent behavior amongst teenagers.[322]

Wearable devices, such as Fitbits,[323] Apple Watches,[324] and others, produce automated data for users to help track their health.[325] These devices have also become evidence in criminal courts.[326] In California, the Fitbit worn by a woman killed in her home was used to argue that her time of death coincided with surveillance footage of

320. *See* Glencorra Borradaile et al., *Whose Tweets are Surveilled for the Police: An Audit of a Social-Media Monitoring Tool via Log Files*, *in* PROC. OF THE 2020 CONF. ON FAIRNESS, ACCOUNTABILITY, AND TRANSPARENCY SESS. 3 (2020), https://arxiv.org/pdf/2001.08777.pdf [https://perma.cc/FY86-YCHY]; *see, e.g.*, Phillips, supra note 3. Consider the prosecution of Roberta Baker for the death of her prematurely born son Elijah; her Facebook messages that included a picture of Elijah were used by the prosecutor to argue her knowledge about her son's medical vulnerability. *See* McFarland, *supra* note 301. Ms. Baker was sentenced to twenty years for failing to get Elijah medical attention sooner. Matthew McFarland, *Baker Gets 20-Year Sentence for Newborn's Death*, DAILY J., https://dailyjournalonline.com/news/local/crime-and-courts/baker-gets-20-year-sentence-for-newborns-death/article_28d4b98a-f89f-5e86-8dde-fe2a10aef7b0.html [https://perma.cc/Z4TQ-3GXK] (Aug. 29, 2019).

321. *See* Borradaile et al., *supra* note 320, at 14–15; *see also Map: Social Media Monitoring by Police Departments, Cities, and Counties*, BRENNAN CTR. FOR JUST. (Jul. 10, 2019), https://www.brennancenter.org/our-work/research-reports/map-social-media-monitoring-police-departments-cities-and-counties [https://perma.cc/9NYK-XZ7U].

322. *See generally* DESMUND UPTON PATTON ET AL., USING NATURAL LANGUAGE PROCESSING AND QUALITATIVE ANALYSIS TO INTERVENE IN GANG VIOLENCE: A COLLABORATION BETWEEN A SOCIAL WORK RESEARCHERS AND DATA SCIENTISTS (2016), https://arxiv.org/ftp/arxiv/papers/1609/1609.08779.pdf [https://perma.cc/XF5Z-6KNQ].

323. *See* Lisa Eadicicco, *I'm a Loyal Apple Watch User, but After Switching to Fitbit, I Found 3 Things I Liked Better and 3 Things I Didn't*, BUS. INSIDER, (Dec 5, 2019), https://buisinessinsider.com/apple-watch-series-5-vs-fitbit-versa-2-features-compared-2019-12 [https://perma.cc/3NSY-ARPY].

324. *See* Kristen V. Brown, *What Happens When the Computer That Keeps You Alive Can Also Put You in Jail?*, GIZMODO (Feb. 14, 2017, 12:27 PM), https://gizmodo.com/what-happens-when-the-computer-that-keeps-you-alive-can-1792236550 [https://perma.cc/F92F-BJH5].

325. *See* Eadicicco, *supra* note 323.

326. *See* Christine Hauser, *Police Use Fitbit Data to Charge 90-Year-Old Man in Stepdaughter's Killing*, N.Y. TIMES (Oct. 3, 2018), https://nytimes.com/2018/10/03/us/fitbit-murder-arrest.html [https://perma.cc/S2AV-BKXD].

her father-in-law's visit.[327] The device detects heartbeat data and the State sought to prove that this data showing her escalated heartbeat was a result of an attack.[328]

Many women enter their menstrual cycle schedules and other reproductive health details into various types of apps.[329] The companies responsible for these apps often sell this data.[330] Officials in the federal immigration system have purchased similar data,[331] and rather than relying on warrants, they have used this data to track immigrants' menstrual cycles in order to monitor for pregnancy.[332] New executive rules prohibiting people seeking visas for the purposes of giving birth on American soil may also inspire additional use of menstrual tracking by the Department of Homeland Security.[333]

Finally, smart home devices—whether they are Alexa, Google Home, smart water meters,[334] or any other smart devices that contain similar information as a search engine—have also been subpoenaed for data recordings contemporaneous with the time and date of a crime.[335] Amazon has sought a patent for developing technology that

327. *See* Lauren Smiley, *A Brutal Murder, a Wearable Witness, and an Unlikely Suspect*, WIRED (Sept. 17, 2019, 6:00 AM), https://wired.com/story/telltale-heart-fitbit-murder/ [https://perma.cc/4MF2-SPPT].

328. *See id.*

329. *See* Hannah Nichols, *The 10 Best Period Tracking Apps*, MED. NEWS TODAY (Jan. 29, 2018), https://medicalnewstoday.com/articles/320758 [https://perma.cc/DE37-WQS3].

330. *See* Baker*, supra* note 251.

331. *See* Jamie Ross, *Trump Administration Using Cellphone App Data to Hunt for Undocumented Immigrants: Report*, DAILY BEAST (Feb. 7, 2020, 8:14 AM), https://thedailybeast.com/trump-administration-uses-your-cellphone-data-for-immigration-enforcement-report [https://perma.cc/H66R-Q34T?type=image].

332. *See* Jennifer Wright, *The U.S. is Tracking Migrant Girls' Periods to Stop Them from Getting Abortions*, HARPER'S BAZAAR (Apr. 2, 2019), https://harpersbazaar.com/culture/politics/a26985261/trump-administrtion-abortion-period-tracking-migrant-women/ [https://perma.cc/6TJT-AHTP].

333. *See id.*; *see also* Ross, *supra* note 331.

334. *See* Grace Manning, Online Contribution, *Alexa: Can You Keep a Secret? The Third-Party Doctrine in the Age of the Smart Home*, AM. CRIM. L. REV. (2019), https://www.law.georgetown.edu/american-criminal-law-review/wp-content/uploads/sites/15/2019/02/56-O-Alexa-Can-You-Keep-a-Secret-The-Third-Party-Doctrine-in-the-Age-of-the-Smart-Home.pdf [https://perma.cc/7XXT-KDQX] ("Indeed, law enforcement in the Bates case obtained data from Bate's smart water meter without a warrant after prosecutors thought he may have used it to hose down blood.").

335. *See id.*; Minyvonne Burke, *Amazon's Alexa May Have Witnessed Alleged Florida Murder, Authorities Say*, NBC NEWS, https://nbcnews.com/news/us-news-amazon-s-

will recommend purchases based on detections of coughs, sneezes, and other symptoms of sickness, suggesting that the technology industry is not deterred by claims of reasonable expectation of privacy of medical information.[336]

Digital devices produce new types of evidence that document not only the things that we do, but also the thoughts that we have.[337] Anti-abortion prosecutors and police—who previously only relied on medical records, doctors, nurses, experts, and perhaps hearsay from people testifying to the pregnant person's mental state—now have access to new tools that give them crucial evidence of what is going through a pregnant person's mind in the weeks and months before their pregnancy ends.[338]

7. Digital data presents the potential for prosecutors and police to circumvent medical staff to surveil pregnant people.

In addition to having new tools documenting a pregnant person's mental state, anti-abortion prosecutors and police can now circumvent the medical staff they previously relied on for reports of suspected terminations.[339] Prosecutors and investigators could potentially subpoena ISP's for the IP addresses of every search for "abortion medication" or "abortion pills" or any other keyword combination.[340] They could make a similar demand from Google or

---

alexa-may-have-witnessed-alleged-florida-murder-authorities-n1075621 [https://perma.cc/2GNH-X4BV] (Nov. 2, 2019, 4:06 PM).

336. *See* Ivan Mehta, *Amazon's New Patent Will Allow Alexa to Detect a Cough or a Cold*, NEXT WEB (Oct. 15, 2018), https://thenextweb.com/artificial-intelligence/2018/10/15/amazons-new-patent-will-allow-alexa-to-detect-your-illness/ [https://perma.cc/V42R-R6UN].

337. *See id.*

338. *See* Baker, *supra* note 251.

339. *See id.*

340. Sean Lyngaas, *DHS Asks Congress for Subpoena Authority to Contact Vulnerable Asset Owners*, CYBERSCOOP (Oct. 9, 2019), https:/cyberscoop.com/dhs-cisa-subpoena-authority-vulnerable-asset-owners/ [https://perma.cc/CM83-6U49] ("The Department of Homeland Security has asked lawmakers for subpoena authority in order to directly contact organizations vulnerable to hacking rather than having to rely on outside parties to communicate with the private sector."); *see also* Sarah Coble, *US Homeland Security Wants to Subpoena ISPs to Hand Over Data*, INFOSECURITY MAG. (Oct. 11, 2019), https://www.infosecurity-magazine.com/news/us-homeland-security-wants-subpoena/ [https://perma.cc/F85E-TN2P] ("The cybersecurity branch of the Department of Homeland Security has requested legal permission from Congress to demand data from internet services providers in a bid to prevent cyber-attacks. The Cybersecurity and Infrastructure Security Agency (CISA) has chosen National Cybersecurity Awareness Month to seek administrative subpoena authority, which will give it the power to compel ISPs to hand over information.").

from certain websites themselves.[341] If the state has resources, they could also purchase the data from electronic health care record companies or data brokers that collect users' internet and purchasing history and sell it to advertisers.[342] Online search engine surveillance, purchasing history, social media communications and wearable technology data is not protected by medical privileges and is sold by online platforms.[343] Investigators could also do keyword searches on all social media posts within their jurisdiction to find users discussing abortion or any other keyword combination.[344] This potential circumvention could lead to new ways for people to be criminalized for abortion-seeking conduct.[345]

341. *See* Katie Hafner & Matt Richtel, *Google Resists U.S. Subpoena of Search Data*, N.Y. TIMES (Jan. 20, 2006), https://www.nytimes.com/2006/01/20/technology/google-resists-us-subpoena-of-search-data.html [https://perma.cc/U4J6-AXBT] ("The Justice Department has asked a federal judge to compel Google, the Internet search giant, to turn over records on millions of its users' search queries as part of the government's effort to uphold an online pornography law."); *see also* Nathan F. Wessler, *How Private is Your Online Search History?*, ACLU (Nov. 12, 2013, 12:04 PM), https://www.aclu.org/blog/national-security/privacy-and-surveillance/how-private-your-online-search-history [https://perma.cc/KLA6-LUSM]; *see also* Arturo Garcia, *Did the Justice Department Demand Facebook Information for 'Anti-Trump Activists'?*, SNOPES (Oct. 8, 2018), https://www.snopes.com/fact-check/justice-department-facebook-anti-trump-activists/ [https://perma.cc/8MEV-S2UD]; *see also* Jacob Brogan, *The Department of Justice Demands Records on Every Visit to Anti-Trump Protest Site DisruptJ20*, SLATE (Aug. 15, 2017, 12:44 PM), https://slate.com/technology/2017/08/department-of-justice-demands-1-3-million-ip-addresses-of-visitors-to-disruptj20.html [https://perma.cc/QQ68-HBBC] ("On Saturday, a judge in the Superior Court of the District of Columbia approved a search warrant that would require DreamHost, DisruptJ20's provider, to turn over a wide range of information about the site and its visitors. In addition to information about the site's creators, the DOJ demands 'logs showing connections related to the website, and any other transactional information, including records of session times and duration.' In short, the government is looking for records of everyone who even visited the site, which is to say it's effectively compiling info on those who showed even a modicum of interest in protesting the administration.").

342. *See* Thomas Brewster, *Explained: Why the Feds Are Raiding Tech Companies for Medical Records*, FORBES (Feb. 9, 2020, 8:35 AM), https://www.forbes.com/sites/thomasbrewster/2020/02/09/explained-why-the-feds-are-raiding-tech-companies-for-medical-records/#1c3e01f649eb [https://perma.cc/CXZ9-3DDP].

343. *See* Laura Harrison, *How Pregnancy Monitoring Technology Contributes to the War on Women*, WASH. POST (July 8, 2019, 6:00 AM), https://www.washington3post.com/outlook/2019/07/08/how-pregnancy-monitoring-technology-contributes-war-women/ [https://perma.cc/QN42-4CBT].

344. *See* Coutts, *supra* note 308.

345. *See* Baker, *supra* note 251.

B. Tech-Assisted Future Criminalization of Abortion Providers.

Pregnant people are not the only ones vulnerable to prosecution and more vulnerable given their digital trails.[346] Rather than initiate prosecutions of pregnant people possessing illegally obtained abortion pills, the federal government has chosen to strategically target the sources of the pills—for now.[347]

1. Providers being investigated and prosecuted.

The Guttmacher 2019 report highlighted the website of Aid Access, an organization founded by Dr. Rebecca Gomperts, that offered misoprostol and mifepristone by mail-order nationwide starting in March 2018.[348] Aid Access reported serving mostly poor and low-income women in states with less abortion access.[349] It caught the attention of the Food and Drug Administration,[350] which issued a cease and desist letter in March 2019.[351] In defiance of the FDA's cease and desist letter, Aid Access has continued to provide access to medication abortions through its online consultation and mail-order program, although many have complained online in past

346. *See supra* note 309 and accompanying text.

347. *See infra* note 356 and accompanying text.

348. *See* JONES ET AL., *supra* note 13, at 10; *see also About Aid Access*, AID ACCESS, https://aidaccess.org/en/page/698649/about-aid-access [https://perma.cc/83TQ-RNPM] (last visited Nov. 4, 2020).

349. *See* JENNA JERMAN ET AL., GUTTMACHER INST., CHARACTERISTICS OF U.S. ABORTION PATIENTS IN 2014 AND CHANGES SINCE 2008, GUTTMACHER INST. 3, 13 (2016), https://www.guttmacher.org/sites/default/files/report_pdf/characteristics-us-abortion-patients-2014.pdf [https://perma.cc/KQ5V-FD4F].

350. Letter from U.S. Food & Drug Admin. to Aidaccess.org (Mar. 8, 2019), https://www.fda.gov/inspections-compliance-enforcement-and-criminal-investigations/warning-letters/aidaccessorg-575658-03082019 [https://perma.cc/9DEE-U7J6]; *see also* Nancy W. Mathewson, *Prohibited Acts and Enforcement Tools*, 65 FOOD & DRUG L.J. 545, 546 (2010).

> FDA has three types of enforcement tools at its disposal—advisory actions, administrative actions, and judicial actions—some established by statute and regulations, while others are a matter of policy. Advisory actions include Warning Letters and untitled letters. Administrative actions include administrative detention, recalls and civil penalties. Judicial actions include seizures, injunctions and criminal prosecutions.

Id.

351. Letter from U.S. Food & Drug Admin., *supra* note 350; *see also* Rebecca Gomperts, *FDA vs Aid Access*, AID ACCESS (Apr. 2019), https://aidaccess.org/en/page/200797/fda-vs-aid-access [https://perma.cc/JX9P-CZDT].

months about their packages not arriving.[352] Dr. Gomperts' arguments in her response to the FDA in May 2019 largely rested on Gomperts' status as a licensed medical professional, the lack of FDA jurisdiction over Gomperts' practice in Austria, and the inclusion of medical consultation via telemedicine prior to the medications being mailed.[353] As of yet, the FDA has not taken additional steps towards prosecuting Gomperts but has delayed the packages pregnant people have ordered with her prescription.[354]

---

352. *See Aid Access, Aid Access Will Continue Providing Abortion Care,* FACEBOOK (May 17, 2019), https://www.facebook.com/permalink.php?story_fbid=59583574 4258420 &id=482314375610558&utm_source=planc&utm_medium=website&utm_campaign =fbaidaccess [https://perma.cc/KTD4-MY6T] (Facebook login required); *see also Aid Access*, REDDIT, https://www.reddit.com/r/abortion/search/?q=aid%20access&restrict _sr=1, [https://perma.cc/3B87-LFXM] (last visited Nov. 4, 2020) (providing forums to discuss and share information about Aid Access).

353. *See* Verified Complaint, Gomperts v. Azar, No. 19-CV-003450DCN (D. Idaho July 13, 2020), 2019 WL 4257409. In September, Aid Access sued FDA officials in federal district court on behalf of itself, Dr. Gomperts, and women who have sought medication abortions through the organization (although none of the women are named, the complaint alleges that 127 of them reside in Idaho). *See id.* at ¶ 44. Gomperts alleged that the FDA restricted the distribution of mifepristone and misoprostol through the restricted distribution system known as Risk Evaluation and Mitigation Strategy (REMS) and the Element to Assure Safe Use (ETASU) program in effect since 2000, creating an undue burden on the rights of women in the United States to terminate unwanted pregnancies. *See id.* at ¶¶ 31–36. Gomperts also alleged that since March 2018, she has prescribed misoprostol and mifepristone to 7,131 women in the United States after her review of their medical history. *See id.* at ¶¶ 43–46. The complaint describes the receipt of the FDA letter on March 8, 2019 and documents that FDA investigators have indeed intercepted approximately three to ten packages from Dr. Gomperts "based upon tracking information for the packages and communications from her patients." *Id.* at ¶¶ 58–65, 68. Her patients have also been contacted by the FDA through letters and visits, although the FDA stated it "generally does not take enforcement action against individuals who [import drugs for personal use]." Sarah McCammon, *European Doctor Who Prescribes Abortion Pills to US Women Online Sues FDA*, NPR, https://www.npr.org/2019/09/09/758871490/euro pean-doctor-who-prescribes-abortion-pills-to-u-s-women-online-sues-fda [https://per ma.cc/2KFE-PV9U] (Sept. 9, 2020, 5:00 PM). Her claims against the FDA included violations of substantive due process (right to privacy), equal protection, and three violations of the Administrative Procedures Act. *See* Verified Complaint, *Gomperts*, No. 19-CV-003450DCN, at ¶¶ 92–110. Gomperts sought multiple injunctions prohibiting the FDA from seizing her patients' medications and prosecuting Gomperts or her patients for the delivery/receipt of misoprostol and mifepristone, in addition to declaratory relief. *See id.* at ¶¶ 20–23. Gomperts' lawsuit was dismissed by the district court on July 13, 2020. Gomperts v. Azar, No. 19-CV-003450DCN, 2020 WL 3963864, at *11 (D. Idaho July 13, 2020).

354. *See* Marie Solis, *The Unbearable Stress of Waiting for Abortion Pills to Come in the Mail*, VICE (Feb. 26, 2020, 12:30 PM), https://www.vice.com/en_us/article/884v7b/

Distinguishable from Aid Access's licensed and physician-supervised program, in June 2019 Wisconsin's US Attorney's office indicted a New York woman, Ursula Wing, (a web-developer with no medical education) for "conspiracy to defraud the United States and causing the introduction of misbranded drugs into interstate commerce," in addition to smuggling and selling misoprostol and mifepristone via mail-order without a license.[355]

From May 2016 through February 2019, Wing mailed over two thousand customers medications by using fake jewelry store packaging and covertly hiding the pills inside the jewelry box, without any advertising.[356] While an attorney told Wing that her business was targeted as a result of the arrest of a Wisconsin man for spiking his girlfriend's water with the abortion medications, she was also potentially targeted by the Federal Government after being identified as the "top-rated" self-abortion kit supplier by Plan C.[357] It could have also been flagged earlier when PayPal stopped allowing her to use its platform to receive payments in April 2018 (likely at the suggestion of federal investigators).[358] Before she was indicted, FDA investigators obtained a search warrant for her apartment and seized computers, phones, iPads, and medication in February 2019.[359] She was indicted in June and later pleaded guilty to conspiracy.[360]

These "underground" networks are more complex than provider-patient relationships.[361] Licensed physicians may also provide the medication abortion kits to unlicensed practitioners who assist

---

aid-access-abortion-pills-stuck-in-customs [https://perma.cc/RYU5-WU38].

355. *Grand Jury Returns Indictments*, U.S. DEP'T OF JUST. (June 27, 2019), https://www.justice.gov/usao-wdwi/pr/grand-jury-returns-indictments-88 [https://perma.cc/U2TY-YXUN].

356. *See* Chelsea Conaboy, *She Started Selling Abortion Pills Online. Then the Feds Showed Up.*, MOTHER JONES, at https://www.motherjones.com/politics/2019/02/she-started-selling-abortion-pills-online-then-the-feds-showed-up/ [https://perma.cc/T6MK-TCBD] (last visited Nov. 3, 2020).

357. *See generally, The Plan C Report Card*, PLAN C, https://plancpills.org/reportcard [https://perma.cc/YDD6-4RJ5] (last visited Nov. 4, 2020).

358. *See* Conaboy, *supra* note 356.

359. *See* Imani Gandy, *New York Woman Faces Up to Eight Years Behind Bars for Selling Abortion Pills Online*, REWIRE NEWS GRP. (Aug. 9, 2019, 4:49 PM), https://rewire.news/ablc/2019/08/09/new-york-woman-faces-up-to-eight-years-behind-bars-for-selling-abortion-pills-online/ [https://perma.cc/H4KM-8356].

360. *See id*.; *see also* Kevin Murphy, *Abortion-Drug Dealer Pleads Guilty, Linked to Grand Rapids Man Accused of Poisoning Pregnant Woman's Drink*, WIS. RAPIDS TRIB. (Mar. 5, 2020, 4:52 PM), https://www.wisconsinrapidstribune.com/story/news/2020/03/05/abortion-pill-dealer-ursula-wing-guilty-case-tied-grand-rapids-man/4966488002/ [https://perma.cc/FC8R-YM48].

361. *See* Presser, *supra* note 38.

women seeking abortions without the protection of medical licenses or doctor-patient privilege.[362] Unlicensed practitioners have conducted research into medication abortion through web-based and web-assisted methods, network connections on social media, and online purchases.[363] While this network's safety depends on members remaining "anonymous and isolated," their online activity places noisy digital trails that could make providers and their patients easily identifiable to law enforcement agencies.[364]

If pregnant people do not have access to abortion clinics and health insurance, do not feel safe going to a clinic, and cannot obtain online prescriptions following a consultation with a licensed physician—e.g., Dr. Gomperts—the only option left is purchasing misoprostol and mifepristone online.[365] One possible consequence of this trend is the exposure of all providers and patients engaged in medication abortion networks (licensed or not) and the online platforms they rely on,[366] to state and federal criminal investigations, or even prosecutions related to conspiracy, mail fraud, and other charges stemming from the sale, possession, or mailing of abortion medications.[367] As previously discussed, Texas advocates have already pushed for a bill targeting providers mailing abortion pills into the state.[368] Some organizations servicing pregnant people have taken their digital security very seriously and should continue to do so for their staff and the people they serve.[369]

---

362. *See id*.

363. *See* Conaboy, *supra* note 356; *see also* Presser, *supra* note 38; *see also infra* note 364 and accompanying text (discussing the need for online providers to remain anonymous and hidden).

364. *See* Presser, *supra* note 38.

365. *See* Claire Cain Miller & Margot Sanger-Katz, *Why America's Abortion Rate Might Be Higher than It Appears*, N.Y. TIMES (Sept. 20, 2019), https://www.nytimes.com/2019/09/20/upshot/abortion-pills-rising-use.html [https://perma.cc/PU2P-PKKZ].

366. *See* Trujillo *supra* note 210, at 642 (discussing 47 U.S.C. § 230 (2018) ("[A] law that criminalize[s] interactive computer services that operate 'with the intent to promote or facilitate the prostitution of another person.'")).

367. *See Grand Jury Returns Indictments, supra* note 355.

368. *See supra* note 145 and accompanying text. The proposed legislation introduced was designed to make mailing abortion pills into Texas a felony. María Méndez, *As More People Search for Abortion Pills Online, Texas Opponents Push to Restrict Access*, DALL. MORNING NEWS (Dec. 2, 2019, 10:00 AM), https://www.dallasnews.com/news/politics/2019/12/02/as-more-people-search-for-abortion-pills-online-texas-opponents-push-to-restrict-access/ [https://perma.cc/B66S-QRZ5].

369. *See, e.g.*, *Terms of Use and Privacy Policy*, AID ACCESS, https://aidaccess.org/en/page/510/terms-of-use-and-privacy-policy [https://perma.cc/6QXE-XLHN] (last visited Nov. 4, 2020).

2. Additional digital forensics techniques that could target providers.

In addition to the digital tracking that makes pregnant people vulnerable, providers should also be aware of other digital forensic techniques historically used by law enforcement to surveil child pornography, prostitution, and other computer crimes.[370]

Traditionally, image tracking by law enforcement has focused on the child sexual abuse image industry, but tracking software has been purchased by the Department of Homeland Security that could be used to track any type of image as it moves throughout the internet,[371] whether the image includes a flyer with information about how to access abortion, a PDF file of the Anarchist's Cookbook,[372] or any other document that the government wants to tag by its hash-value to trace.[373] "Hash-value matching is a binary authentication method that can scan billions of digital communications in seconds for evidence of contraband."[374] Software systems like the Child Rescue Coalition[375] database generate leads for law enforcement to follow by scanning exchanges of information for these hash-values.[376]

Prosecutors have relied on these systems to prosecute hundreds of people accused of distributing or possessing child pornography despite inconsistencies with the outcomes, for example, the images associated with an IP address were not found on the hard drive owned by the accused person.[377] When faced with court orders to share access to these systems with defense teams, prosecutors prefer

370. *See generally* Trujillo, *supra* note 210, at 625–49 (discussing various computer crimes, law enforcement tactics used to combat the crimes, and issues concerning the crimes).

371. United States v. Shipton, No. 18-cr-202-PJS-KMM, 2019 WL 5330928, at *7–8 (D. Minn. Sept. 11, 2019), *report and recommendation adopted*, No. 18-CR-0202 (PJS/KMM), 2019 WL 5305573 (D. Minn. Oct. 21, 2019).

372. *See* Denae Kassotis, Note, *The Fourth Amendment and Technological Exceptionalism After* Carpenter*: A Case Study on Hash-Value Matching*, 29 FORDHAM INTELL. PROP. MEDIA & ENT. L.J. 1243, 1249–51 (2019).

373. *See id.*

374. *Id.* at 1243.

375. *Our Work*, CHILD RESCUE COAL., https://childrescuecoalition.org/our-work/ [https://perma.cc/GQ9F-3CGV] (last visited Nov. 4, 2020).

376. United States v. Shipton, No. 0:18-cr-202-PJS-KMM, 2019 WL 5330928, at *6–7 (D. Minn. Sept. 11, 2019), *aff'd*, No. 18-CR-0202 (PJS/KMM), 2019 WL 5305573 (D. Minn. Oct. 21, 2019).

377. Jack Gillum, *Prosecutors Dropping Child Porn Charges After Software Tools Are Questioned*, PROPUBLICA (Apr. 3, 2019, 5:00 AM), https://www.propublica.org/article/prosecutors-dropping-child-porn-charges-after-software-tools-are-questioned [https://perma.cc/KBW5-X89S].

to drop the charges or accept a lesser plea, even with protective orders allowing access to attorneys and experts only.[378] This system could be deployed to detect informational flyers about medication abortion, obtaining abortions across state lines, and other abortion options being distributed online through electronic communication or social media.[379]

Another type of forensic technique used by law enforcement—typically in the context of child pornography investigations—is known as the "honeypot."[380]

> "A honeypot or deception host is a designated area within a computer system or network that has been designed specifically with the expectation that it will be attacked by unauthorized users, whether internal or external to the organization operating the honeypot."
>
> . . . Honeypots are essentially passive decoys or copies of target websites. Honeypots provide law enforcement with the ability to capture "detailed and contemporaneous forensic evidence" about the bees that took the bait.[381]

Once the bait has been taken, law enforcement can circumvent the need to subpoena IP addresses from a website or ISP under these circumstances as well by obtaining direct access to the IP addresses.[382] In the abortion context, law enforcement could set up a fake abortion advocate website that collects IP addresses and other information aimed at charging people for taking steps towards getting an abortion or assisting someone in getting an abortion.[383]

Websites hosting classified ads or otherwise facilitating in sex trafficking now face new criminal and civil liability, driving both consensual and coerced sex workers offline and back onto the streets

---

378. *See id.*
379. *See supra* notes 371–78 and accompanying text.
380. Whitney J. Gregory, Comment, *Honeypots: Not for Winnie the Pooh but for Winnie the Pedo — Law Enforcement's Lawful Use of Technology to Catch Perpetrators and Help Victims of Child Exploitation on the Dark Web*, 26 GEO. MASON L. REV. 259, 261 (2018).
381. *Id.* at 278–79 (footnotes omitted) (quoting Ian Walden & Anne Flanagan, *Honeypots: A Sticky Landscape?*, 29 RUTGERS COMPUT. & TECH L.J. 317, 317–18 (2003)).
382. *See id.* at 283–88.
383. *See id.* at 278–79.

to find customers.[384] FOSTA/SESTA[385] removes Section 230 immunity,[386] which previously protected platforms from liability for the content on their sites and as a result, many sex workers relying on web platforms to find clients were removed from Instagram, had their advertisements removed, and their PayPal accounts deactivated.[387] "Eliminating Section 230 immunity also restricts freedom of speech for consensual sex workers seeking safe work because ISPs that fear increased prosecution avoid liability by removing posting capabilities entirely."[388] Consequently, "FOSTA/SESTA has thus forced consensual sex workers to return to work on the streets absent any online platforms willing to host their advertisements."[389] Websites like YouTube and social media outlets like Facebook and Twitter have already censored organizations that provide online information about abortion.[390] Conservatives in Congress could theoretically attempt to de-platform abortion providers with legislation similarly

384. Data & Society Research Institute, *Future Perfect Session 2: Voight-Kampff Tests*, YOUTUBE (July 5, 2018), https://www.youtube.com/watch?v=1xlwaHHAvac&feature=youtu.be.

385. Allow States and Victims to Fight Online Sex Trafficking Act of 2017, Pub. L. No. 115–164, 132 Stat.1253 (2018) (codified as amended at 18 U.S.C. § 2421A).

386. Data & Society Research Institute, *supra* note 384 (relevant discussion beginning at 31:00).

387. *Id.*; *see also* Heidi Tripp, Comment, *All Sex Workers Deserve Protection: How FOSTA/SESTA Overlooks Consensual Sex Workers in an Attempt to Protect Sex Trafficking Victims*, 124 PENN ST. L. REV. 219, 235 (2019).

388. Tripp, *supra* note 387, at 234.

389. *Id.*; *see also* Melissa Gira Grant, *Broad Anti-Trafficking Law Faces its First Constitutional Challenge*, THE APPEAL (June 28, 2018), https://theappeal.org/broad-anti-trafficking-law-faces-its-first-constitutional-challenge [https://perma.cc/HRD2-FF6F] (discussing the lawsuit challenging constitutionality of SESTA/FOSTA).

390. *On the Blocking of Abortion Rights Websites: Women on Waves & Women on Web*, OPEN OBSERVATORY OF NETWORK INTERFERENCE, https://ooni.org/post/2019-blocking-abortion-rights-websites-women-on-waves-web [https://perma.cc/QUD6-SVL4] (last visited Nov. 4, 2020) ("In May 2017, Women on Web tweeted that their Facebook page was unpublished. Facebook reportedly censored the Women on Web page (which helped women obtain abortion pills) citing its policy against the 'promotion or encouragement of drug use'. Their page though was only temporarily unpublished, as Facebook restored access to it soon thereafter. This was not the first time that Women on Web experienced censorship on Facebook. In January 2012, Facebook deleted an image from the page of Dr. Rebecca Gomperts (the founder and director of Women on Web) which consisted of text instructions on how to safely induce an abortion using medication. In addition to Facebook censorship, Women on Web have reportedly experienced censorship by Twitter and YouTube as well. In January 2015, Twitter temporarily disabled the possibility to link to womenonweb.org or to tweet a link to the website. In January 2018, YouTube temporarily removed the video channels from Women on Waves and Women on Web, both of which contained animations with information about safe ways to do an abortion with medicine.").

carving out exceptions to Section 230 immunity, although like FOSTA/SESTA would be subject to First Amendment challenges.[391]

Finally, providers should be aware of all location-tracking surveillance available to law enforcement.[392] That includes the cell phone towers discussed above,[393] automatic license plate readers,[394] cell-site simulators,[395] Bluetooth beacons,[396] and EZ-Pass like devices.[397] These devices could be used to track movements of specific people and to detect patterns of movement back and forth across state lines.[398]

Understandably, continuing to engage with technology after researching and reading about all the new ways digital and surveillance devices track our thoughts and movements can be intimidating.[399] Fortunately, there are movements to protect our data that we can connect with, members of various movements engaging with the challenges of surveillance technology, steps we can take to protect our privacy in our digital engagement, and litigation and

391. *See* Marguerite A. O'Brien, Note, *Free Speech or Slavery Profiteering?: Solutions for Policing Online Sex-Trafficking Advertisement*, 20 VAND. J. ENT. & TECH. L. 289, 299–300 (2017).

392. *See supra* notes 20–21, 178 and accompanying text.

393. *See supra* notes 213–14 and accompanying text.

394. *Automated License Plate Readers (ALPRs)*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/automated-license-plate-readers-alpr [https://perma.cc/22KQ-JXVZ] (Aug. 28, 2017).

395. *Cell-Site Simulators/IMSI Catchers*, ELEC. FRONTIER FOUND., https://www.eff.org/pages/cell-site-simulatorsimsi-catchers [https://perma.cc/CB6V-3J5B] (Aug. 28, 2017).

396. *See Indoor Positioning, Tracking and Indoor Navigation with Beacons*, INFSOFT, https://www.infsoft.com/technology/positioning-technologies/bluetooth-low-energy-beacons [https://perma.cc/7VL2-Z26X] (last visited Nov. 4, 2020); *see Six Ways to Use Bluetooth Beacons for People and Asset Tracking*, TEAM SOFTWARE (Nov. 26, 2019), https://teamsoftware.com/blog/2019/11/26/six-ways-to-use-bluetooth-beacons-for-people-and-asset-tracking/ [https://perma.cc/3625-D7KJ]; *see* Christopher McFadden, *Are You Being Tracked by Bluetooth Beacons While Shopping?*, INTERESTING ENG'G (June 20, 2019), https://interestingengineering.com/are-you-being-tracked-by-bluetooth-beacons-while-shopping [https://perma.cc/6KGM-VRFM].

397. Becky Akers, *Congestion Pricing: The Road to the Surveillance State*, FOUND. FOR ECON. EDUC. (Jan. 1, 2008), https://fee.org/articles/congestion-pricing-the-road-to-the-surveillance-state/ [https://perma.cc/B4WF-473U].

398. *See* Kareem Fahim et al., *Cellphone Monitoring is Spreading with the Coronavirus. So is an Uneasy Tolerance of Surveillance*, WASH. POST (May 2, 2020, 4:12 PM), https://www.washingtonpost.com/world/cellphone-monitoring-is-spreading-with-the-coronavirus-so-is-an-uneasy-tolerance-of-surveillance/2020/05/02/56f14466-7b55-11ea-a311-adb1344719a9_story.html [https://perma.cc/ZLR7-F8YN].

399. *See supra* notes 392–98 and accompanying text.

policy strategies we can deploy to control the damage our digital devices are capable of inflicting upon us.[400]

IV. "POWER, NOT PARANOIA"[401]

This all feels overwhelming, and it is. But there are organizing, corporate accountability, legal, and policy strategies being developed with creativity, resilience, and research.[402] There are other social justice movements, for example, in immigration and police surveillance spaces, that have woven digital privacy, data protection, and state surveillance into their community organizing work.[403] Like these movements, the reproductive justice movement will also need to confront the challenges technology poses and create new protections for our communities to maintain their decisional-privacy around reproductive health in digital spaces and safely continue to rely on technology to access important information about abortion.[404]

A. Organizing & Corporate Accountability.

"Power not paranoia" is a framework developed through the lens of protecting communities in Los Angeles from police surveillance by the Stop LAPD Spying Coalition.[405] The framework acknowledges "that the violence we live through does impact our mental health . . . because we are experiencing the impacts of a culture of fear and want to transform the impact."[406] Building on this framework, coalitions like the Our Data Bodies Project—which the Stop LAPD Spying Coalition is a part of—have developed out of historically oppressed communities organizing around digital data collection and human rights.[407] Their research has resulted in tools like the Digital Defense Playbook[408], community reports, and popular educational materials[409]

400. *See infra* notes 402–03, 405 and accompanying text.
401. Kim M. Reynolds, *Power Not Paranoia: An Oral History*, OUR DATA BODIES https://www.odbproject.org/2019/01/18/power-not-paranoia-an-oral-history/ [https://perma.cc/3PNF-MWG6] (last visited Nov. 4, 2020).
402. *See* RUHA BENJAMIN, RACE AFTER TECHNOLOGY 163, 166, 168, 171–72, 174–76, 184–85, 189 (2019) (ebook).
403. *See id.*
404. *See infra* notes 434–39, 453 and accompanying text.
405. Reynolds, *supra* note 401.
406. *Id.*
407. *What We Are Doing*, OUR DATA BODIES, https://www.odbproject.org/about/what-we-are-doing/ [https://perma.cc/23GE-PTCW] (last visited Nov. 4, 2020).
408. SEETA PEÑA GANGADHARAN ET AL., DIGITAL DEFENSE PLAYBOOK: COMMUNITY POWER TOOLS FOR RECLAIMING DATA (2018), https://www.odbproject.org/wp-content/uploads/2019/03/ODB_DDP_HighRes_Single.pdf [https://perma.cc/4DJE-HHMB].

like six "Tips for Protecting Our Data."[410] These types of educational tools inform people about how to apply privacy settings on their devices to minimize their exposure to corporate and state surveillance.[411]

Recent organizing efforts in criminal justice,[412] immigration,[413] education,[414] public health,[415] and poverty movements[416] have pushed back against the new opportunities for state intrusions created by technology.[417] For example, the Community Justice Exchange collaborated with the Movement Alliance Project (MAP) to develop an organizer's toolkit designed to help bail reform organizers push back against algorithm-based decision-making tools reliant upon data collected in the criminal justice system.[418] When Philadelphia's

409. *Tools*, OUR DATA BODIES, odbproject.org/tools/ [https://perma.cc/GG43-Y4MX] (last visited Nov. 3, 2020).

410. *Our Data Bodies Project*, *supra* note 94.

411. *See* GANGADHARAN ET AL., *supra* note 408, at 35–37 (describing activity to educate workshop participants about protecting their data trails).

412. *See, e.g.*, *Mapping Pretrial Injustice: A Community Driven Database*, MAPPING PRETRIAL RISK, pretrialrisk.com (last visited Nov. 22, 2020) [https://perma.cc/N946-FLY5].

413. *See, e.g.*, MIJENTE ET AL., TAKE BACK TECH: HOW TO EXPOSE AND FIGHT SURVEILLANCE TECH IN YOUR CITY 2 (2019), https://mijente.net/wp-content/uploads/2019/07/Tech-Policy-Report_v4LNX.pdf [https://perma.cc/FNL5-3NDA].

414. *See, e.g.*, Carrie Pomeroy, *How Community Members in Ramsey County Stopped a Big Data Plan from Flagging Students as At-Risk*, TWIN CITIES DAILY PLANET (Feb. 20, 2019), https://www.tcdailyplanet.net/how-community-members-in-ramsey-county-stopped-a-big-data-plan-from-flagging-students-as-at-risk/ [https://perma.cc/DK3D-AR6X].

415. *See, e.g.*, Colin Lecher, *What Happens When an Algorithm Cuts Your Health Care*, THE VERGE (Mar. 21, 2018, 9:00 AM), https://www.theverge.com/2018/3/21/17144260/healthcare-medicaid-algorithm-arkansas-cerebral-palsy [https://perma.cc/B2R4-4PKU]; Legal Aid of Arkansas, Inc., *Fighting the 4,000 Cuts: Tammy Dobbs*, FACEBOOK (Aug. 17, 2017), https://www.facebook.com/arlegalaid/videos/1438194976257716/.

416. *See, e.g.*, Ryan Felton, *Michigan Unemployment Agency Made 20,000 False Fraud Accusations*, THE GUARDIAN (Dec. 18, 2016), https://www.theguardian.com/us-news/2016/dec/18/michigan-unemployment-agency-fraud-accusations [https://perma.cc/6WK2-AX9W]; *The SyRI Case: A Landmark Ruling for Benefits Claimants Around the World*, PRIV. INT'L (Feb. 24, 2020), https://privacyinternational.org/news-analysis/3363/syri-case-landmark-ruling-benefits-claimants-around-world [https://perma.cc/VQ7Z-VQ65].

417. *See infra* notes 418–19 and accompanying text.

418. CMTY. JUST. EXCH., AN ORGANIZER'S GUIDE TO CONFRONTING PRETRIAL RISK ASSESSMENT TOOLS IN DECARCERATION CAMPAIGNS 2, 4 (2019), https://static1.squarespace.com/static/5e1f966c45f53f254011b45a/t/5e35a639a96d977ad27f3ff0/15805742

court system wanted to introduce risk assessment tools into their court process, MAP—along with a coalition of bail reform organizers—successfully stalled its approval and publicly organized against its use, even convincing the local prosecutor to oppose it.[419]

Organizations like Just Futures Law and Mijente—a Latinx and Chicanx movement for "justice and self-determination for *all* people"—produced a joint report identifying the technology companies supporting Immigration and Customs Enforcement (ICE),[420] created graphics explaining the networks,[421] created petitions to companies like Amazon,[422] organized walk-outs by tech workers,[423] and protested under the rally cry (and hashtag) "#NoTechForICE".[424] Further, the Electronic Frontier Foundation, a civil liberties organization, has facilitated a vast network of grassroots organizations across the country around technology issues.[425] Its website hosts a vast amount of knowledge, training, web tools, and other resources for organizers, lawyers, and policy advocates working across multiple movements.[426] One important

68825/CJE_PretrialRATGuide_FinalDec2019Version.pdf [https://perma.cc/L79W-FUYK].

419. *See* Paige Gross, *Pennsylvania's Controversial Risk-Assessment Tool Was Just Approved*, TECHNICAL.LY PHILLY, https://technical.ly/philly/2019/09/06/pennsylvanias-controversial-sentencing-risk-assessment-tool-was-just-approved/ [https://perma.cc/Q78P-RU4H] (Sept. 9, 2019, 4:21 PM).

420. *The J Is for Justice*, MIJENTE, https://mijente.net/our-dna/ [https://perma.cc/DS9F-6EAW] (emphasis added) (last visited Nov. 4, 2020); *New Report Exposes Tech & Data Companies Behind ICE*, MIJENTE (Oct. 23, 2018), https://mijente.net/2018/10/whos-behind-ice-the-tech-companies-fueling-deportations/ [https://perma.cc/ZKX3-BZCG] (detailing joint report).

421. Mijente (@ConMijente), TWITTER (July 11, 2019, 6:30 PM), https://twitter.com/ConMijente/status/1149445902215630849 [https://perma.cc/8NPT-X9EV].

422. *Tech Companies: Stop Powering ICE During Coronavirus!*, #NOTECHFORICE, https://notechforice.com/corona/ [https://perma.cc/QM3N-XBRN] (last visited Nov. 4, 2020).

423. *See* Lauren Kaori Gurley, *Tech Workers Walked Off the Job After Software They Made Was Sold to ICE*, VICE (Oct. 31, 2019, 4:11 PM), https://www.vice.com/en_us/article/43k8mp/tech-workers-walked-off-the-job-after-software-they-made-was-sold-to-ice [https://perma.cc/QJC9-3H7H].

424. Hannah Denham, *'No Tech for ICE': Protesters Demand Amazon Cut Ties with Federal Immigration Enforcement*, WASH. POST (July 12, 2019, 3:45 PM), https://www.washingtonpost.com/business/2019/07/12/no-tech-ice-protesters-demand-amazon-cut-ties-with-federal-immigration-enforcement/ [https://perma.cc/2TZT-TBQH].

425. *See About EFF*, ELEC. FRONTIER FOUND., https://www.eff.org/about [https://perma.cc/34KT-99SP] (last visited Nov. 4, 2020).

426. *See Our Work*, ELEC. FRONTIER FOUND., https://www.eff.org/updates [https://perma.cc/FF25-28R6] (last visited Nov. 4, 2020) (listing available resources).

consideration for digital security planning for pregnant people, abortion providers, and abortion assisters is that the amount of privacy protection we each should employ is not gauged by how exposed one is to criminal prosecution in a personal capacity, but by how exposed the most vulnerable person in our network is.

Data for Black Lives (DBL) is another group of "activists, organizers, and mathematicians committed to the mission of using data science to create concrete and measurable change in the lives of Black people."[427] When parents and grassroots organizers in St. Paul, Minnesota wanted to stop a data collection and sharing agreement by the education and juvenile justice systems to flag "at-risk" youth, Data for Black Lives supported local organizers at an educational summit with a local group named the Coalition to Stop Cradle to Prison Algorithms.[428] In addition to supporting local grassroots efforts to help them combat government arguments for data surveillance, Data for Black Lives also holds conferences to build bridges between grassroots organizational efforts and academic communities concerned about data.[429] Other convenings, such as the Internet Freedom Festival[430] and the Allied Media Conference[431] also support networking across various movements impacted by new surveillance technology.[432]

Many movements have had to confront the impact of technology in their fights for justice and some have even found allies in the technology space with whom they share organizing strategies and elevate efforts to conquer their communities' struggles.[433]

427. *About Us*, DATA FOR BLACK LIVES, https://d4bl.org/about.html [https://perma.cc/RVM3-JGJA] (last visited Nov. 4, 2020).
428. *See* Pomeroy, *supra* note 414.
429. *See Programs*, DATA FOR BLACK LIVES, https://d4bl.org/programs.html [https://perma.cc/EY8K-83XU] (last visited Nov. 4, 2020); *see also Events*, DATA FOR BLACK LIVES, https://d4bl.org/events.html [https://perma.cc/XVW2-6BKQ] (last visited Nov. 4, 2020).
430. INTERNET FREEDOM FESTIVAL, https://internetfreedomfestival.org/ [https://perma.cc/ZGN7-MBYC] (last visited Nov. 4, 2020).
431. *About*, ALLIED MEDIA PROJECTS, https://www.alliedmedia.org/about.story [https://perma.cc/H8YG-UR7D] (last visited Nov. 8, 2020).
432. *See* sources cited *supra* notes 430–31.
433. *See generally Programs*, *supra* note 429.

B. Legal

There are both affirmative and defensive litigation strategies potentially available.[434] As discussed above, in addition to connecting with advocates like the National Advocates for Pregnant Women and If/When/How—who can frame legal strategies in the larger context of reproductive justice[435] and organizers that can harness political pressure to dismiss charges[436]—defense attorneys should challenge the scope of digital searches by law enforcement by arguing they are *Carpenter*-like violations, whether they are done pursuant to a warrant or based on consent.[437] ACLU's Speech, Privacy, and Technology Project has been monitoring post-*Carpenter* decisions, submitting amicus briefs, and advocating for a broad interpretation of *Carpenter's* protections.[438] The National Association of Criminal Defense Lawyers has also initiated the Fourth Amendment Project, which entails consulting, co-counseling, and training defense attorneys about surveillance technology and other data-driven tools used in the criminal justice system.[439]

Lawyers must also counsel clients about the risks of using their digital devices to communicate and search for information.[440] There are many guides to digital privacy online, like those listed above,[441] that lawyers should make available to their clients while counseling them about their exposure if they have already used a digital device.[442]

---

434. *See generally About NAPW*, NAT'L ADVOCS. FOR PREGNANT WOMEN, http://advocatesforpregnantwomen.org/main/about_us/about_us.php [https://perma.cc/UD34-PSD8] (last visited Nov. 3, 2020).

435. IF/WHEN/HOW: LAWYERING FOR REPRODUCTIVE JUSTICE, https://ifwhenhow.org [https://perma.cc/E64W-725X] (last visited Nov. 4, 2020); *About NAPW*, *supra* note 434.

436. *See supra* notes 2–11, 438–39 and accompanying text; *see also Tell DA Scott Colom: Drop the Charges Against Latice Fisher*, COLOR OF CHANGE, https://act.colorofchange.org/sign/no-charges-against-latice [https://perma.cc/KG7K-XTQT] (last visited Nov. 4, 2020) (organizing petitions to reduce Ms. Fisher's bail and pressure District Attorney to drop charges).

437. For a detailed discussion of Carpenter, see *supra* Section III.A.4.i.

438. Nathan Freed Wessler, *The Supreme Court's Most Consequential Ruling for Privacy in the Digital Age, One Year In*, ACLU (June 28, 2019, 4:30 PM), https://www.aclu.org/blog/privacy-technology/location-tracking/supreme-courts-most-consequential-ruling-privacy-digital [https://perma.cc/Y7VQ-HAD9].

439. *Fourth Amendment*, NAT'L ASS'N OF CRIM. DEF. LAWS., https://www.nacdl.org/Landing/FourthAmendment [https://perma.cc/MG9D-GYEA] (last visited Nov. 4, 2020).

440. NACDLvideo, *supra* note 61.

441. *See supra* notes 408–09, 426 and accompanying text.

442. *See generally Fourth Amendment*, *supra* note 439.

There may also be affirmative litigation opportunities in cities and states with privacy protections.[443] States like Arizona and New Jersey, which have constitutional privacy protections,[444] were joined in the digital era by states like California, discussed in more depth below,[445] which enacted new privacy protections specifically designed to address new digital invasions.[446] Additionally, New Hampshire, Virginia, Illinois, Washington, and New York have also introduced bills similar to California to authorize private rights of action against technology companies for privacy violations.[447]

These new private right of action bills could give litigators more opportunities to fight for privacy protections for pregnant people seeking privacy in their decision-making regarding their reproductive health.[448]

C. Policy

Attempts at regulating data sharing have begun at both federal and state levels.[449] In 2018, California passed the strongest privacy legislation.[450] The California Consumer Privacy Act of 2018 gives

443. Libbie Canter et al., *State Legislatures Are Off to the Privacy Races, with New Hampshire in the Lead*, COVINGTON (Jan. 10, 2020), https://www.insideprivacy.com/ccpa/state-legislatures-are-off-to-the-privacy-races-with-new-hampshire-in-the-lead/ [https://perma.cc/LZT4-PQXX].

444. State v. Mixton, 447 P.3d 829, 842–43 (Ariz. Ct. App. 2019) (holding under Arizona state constitution protection of "private affairs;" "internet users generally have an expectation of privacy in their subscriber information. . . . Warrantless government collection of this information from an internet service provider or similar source thus constitutes a significant and unwarranted intrusion into a person's private affairs—an intrusion our constitution unambiguously prohibits."); State v. Reid, 945 A.2d 26, 33 (N.J. 2008) (affirming suppression under state constitution for warrantless request to ISP for IP address subscriber information).

445. *See infra* notes 446–51 and accompanying text.

446. Jill Cowan & Natasha Singer, *How California's New Privacy Law Affects You*, N.Y. TIMES (Jan. 3. 2020), https://www.nytimes.com/2020/01/03/us/ccpa-california-privacy-law.html [https://perma.cc/3C4V-R4MG].

447. Canter et al., *supra* note 443.

448. *Id.*

449. Wessler, *supra* note 438; *see also* Letter from 18MillionRising.org et al., to Axon AI Ethics Board (Apr. 26, 2018) (on file with The Leadership Conference on Civil & Human Rights), http://civilrightsdocs.info/pdf/policy/letters/2018/Axon%20AI%20Ethics%20Board%20Letter%20FINAL.pdf [https://perma.cc/X382-EJBT] (signed by organizations like Upturn, Electronic Frontier Foundation, ACLU's Speech, Privacy and Tech Project, AI Now, and Data & Society that contributed research to identifying the new privacy needs presented by digital tracking).

450. Jon Brodkin, *California Approves Privacy Rules Opposed by ISPs and Tech Companies*, ARS TECHNICA (June 28, 2018, 5:32 PM), https://arstechnica.com/tech-

consumers the right to know what personal information ("PI") is being collected about them and whether their PI is being sold and to whom; the right to access their PI; the right to delete PI collected from them; the right to opt-out or opt-in to the sale of their PI, depending on the age of the consumer; and the right to equal service and price, even if they exercise such rights.[451] As discussed above, state constitutional privacy provisions in Arizona, New Jersey, and other states can protect people accused of crimes based on digital device evidence, even when federal third-party doctrine does not.[452] New laws have also been enacted at the state and city levels to protect individuals' personal information gathered from biometric data.[453]

At the federal level, the Online Privacy Act "would create a new federal agency, the Digital Privacy Agency, to enforce privacy rights."[454] Another bill, the Algorithmic Accountability Act, would enable the Federal Trade Commission to conduct investigations into data protections for data used by algorithms in the public sector.[455] Facial recognition technology and the data those systems collect from our faces is also a target of pending legislation.[456] One weakness many of these laws share, however, is broad carve-outs for "public safety" or, in other words, law enforcement.[457] None of the new digital privacy legislation would heighten the standard for what a

---

policy/2018/06/california-approves-privacy-rules-opposed-by-isps-and-tech-companies/ [https://perma.cc/33KJ-M6J4].

451. *Id.*; Cowan & Singer, *supra* note 446; *Today's Law as Amended*, CAL. LEGIS. INFO. (Nov. 08, 2018), https://leginfo.legislature.ca.gov/faces/billCompareClient.xhtml?bill_id=201720180AB375&showamends=false# [https://perma.cc/FNX6-K5LS].

452. *See supra* notes 215–16, 443–46 and accompanying text.

453. *See, e.g.*, 740 ILL. COMP. STAT. ANN. 14/15 (West 2020). San Francisco, California, Oakland, California, and Somerville, Massachusetts have all enacted facial recognition bans. Shirin Ghaffary, *How Facial Recognition Became the Most Feared Technology in the US*, VOX (Aug. 9, 2019, 4:00 PM), https://www.vox.com/recode/2019/8/9/20799022/facial-recognition-law [https://perma.cc/AZ22-NXNS].

454. Kate Cox, *New Bill Would Create Digital Privacy Agency to Enforce Privacy Laws*, ARS TECHNICA (Nov. 5, 2019, 5:07 PM), https://arstechnica.com/tech-policy/2019/11/new-bill-would-create-digital-privacy-agency-to-enforce-privacy-rights/ [https://perma.cc/6W4E-9LLE].

455. Algorithmic Accountability Act, H.R. 2231, 116th Cong. (2019).

456. *See* Ghaffary, *supra* note 453.

457. *See, e.g.*, N.Y. POLICE DEP'T, PATROL GUIDE: USE OF DEPARTMENT UNMANNED AIRCRAFT SYSTEM (UAS) (2018), https://www1.nyc.gov/assets/nypd/downloads/pdf/public_information/public-pguide2.pdf#page=687 [https://perma.cc/6WEL-853U] (detailing carve-outs under Section 212-124).

prosecutor or sheriff would need to present to obtain the search history for a woman suspected of terminating her own pregnancy.[458]

Other policy recommendations include limiting data retention and use from health-related websites[459] similar to prohibitions in Article 9 of the European General Data Protection Regulation (GDPR), which protects "data concerning health or data concerning a natural person's sex life or sexual orientation[.]"[460] This type of regulation may protect reproductive health data more consistently than digital privacy laws with public safety exceptions.[461]

There are also new regulations that may compromise Americans' digital privacy related to their medical records.[462] A new federal rule requires health providers to share medical information with third-party apps (e.g., Apple's Health Records with patient authorization) but offers no protection from the health records shared with those companies from being further transferred to insurance companies, employers, or law enforcement.[463] Legislation has also been introduced to require private companies that sell tools to the public sector for use in the criminal justice system to share their source code and other information about how systems are created with defense attorneys.[464]

---

458. *See generally* Eric Litke, *Fact Check: Did Senators Vote to Allow Access to Web History? Only for Counterterrorism*, USA TODAY, https://www.usatoday.com/story/news/factcheck/2020/05/21/fact-check-senate-didnt-ok-warrantless-access-internet-history/5236880002 [https://perma.cc/K3K8-4PQA] (May 27, 2020, 4:18 PM) (discussing the Senate's vote to allow federal agencies access to search history without a warrant). The policy recommendation by Upturn to ban consent searches on digital devices, in contrast, would have prevented Ms. Fisher's digital device from being confiscated and analyzed without a judicial warrant. *See* KOEPKE ET AL., *supra* note 148, at 59–61.

459. Tim Libert, *Privacy Implications of Health Information Seeking on the Web*, TIMOTHY LIBERT (Mar. 2015), https://timlibert.me/pdf/Libert-2015-Health_Privacy_on_Web.pdf [https://perma.cc/L69Q-A9JL].

460. Council Regulation 2016/679, art. 9, 2016 O.J. (L 119) 1.

461. *See id.*

462. *E.g.*, Natasha Singer, *When Apps Get Your Medical Data, Your Privacy May Go with It*, N.Y. TIMES (Sept. 3, 2019), https://www.nytimes.com/2019/09/03/technology/smartphone-medical-records.html [https://perma.cc/C8DS-H4GY].

463. *See id.*

464. Tim Cushing, *Rep. Mark Takano Introduces Bill That Would Keep Companies from Blocking Defendants' Access to Evidence*, TECHDIRT (Sept. 25, 2019, 7:59 PM), https://www.techdirt.com/articles/20190923/18322143049/rep-mark-takano-introduces-bill-that-would-keep-companies-blocking-defendants-access-to-evidence.shtml [https://perma.cc/9DGH-THSH].

Some policy recommendations are aimed at technology companies directly, encouraging them to set the highest level of privacy as defaults and encouraging engineers to figure out ways to filter data that has medically sensitive information and prevent its redistribution.[465] Search engines have also taken steps to deter the large volume of law enforcement search history requests by proposing to charge per request.[466]

Problematically, it is not clear that even these much needed solutions would address the broad power that the government has to administratively subpoena information from these search engines.[467] That is not a reason to despair, but a reason to organize and incorporate these very real concerns into new legislation limiting what police and prosecutors can access from third parties about medically relevant information collected by digital devices.[468]

CONCLUSION

Controlling pregnant people's bodies and decisions about their pregnancy have long been the goal of many people in power.[469] Never before have they had such a strong arsenal of surveillance tools with which to do it.[470] Whether it is being able to peer into our digital diaries—by seizing digital devices and search histories, tracking physical movements, or identifying people through biometrics—the amount of digital, biometric, and genetic data tracking the government is currently capable of changes the nature of every conversation about social justice, especially in an era lurching backwards towards criminalizing pregnancy outcomes.[471]

These new unregulated technological developments, in combination with the potential increase in the criminalization of pregnancy and abortion, will create life-long devastating penalties for people seeking autonomy over their decisions related to their reproductive health.[472] As we strategize solutions for new versions of old problems presented by surveillance technology, we must

---

465. *See* Libert, *supra* note 459, at 75.
466. Gabriel J.X. Dance & Jennifer Valentino-DeVries, *Have a Search Warrant for Data? Google Wants You to Pay*, N.Y. TIMES (Jan. 24, 2020), https://www.nytimes.com/2020/01/24/technology/google-search-warrants-legal-fees.html [https://perma.cc/W5VG-EADU].
467. *See supra* notes 339–43 and accompanying text.
468. *See supra* notes 459–66 and accompanying text.
469. *See supra* Section II.A.
470. *See supra* Part III.
471. *See supra* Section III.A.
472. *See supra* notes 18–34 and accompanying text.

nevertheless maintain the fundamental goals of deconstructing racism, misogyny, and patriarchy.[473]

473. *See supra* Part I.